fa – fd

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.

Command Default

Failover is disabled.

Command Modes

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

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

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:

```
ciscoasa(config)# no failover
ciscoasa(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.

Command Default

No default behavior or values.

Command Modes

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

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

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:

```
ciscoasa# failover active group 1
```

Related Commands

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

failover cloud authentication

To allow the ASA virtual to authenticate with Microsoft Azure using a Service Principal, use the **failover cloud authentication** command in global configuration mode. To disable Microsoft Azure authentication, use the **no** form of this command.

failover cloud authentication { **application-id** *appl-id* | **directory-id** *dir-id* | **key** *secret-key* }
no failover cloud authentication { **application-id** *appl-id* | **directory-id** *dir-id* | **key** *secret-key* [**encrypt**] }

Syntax Description

application-id *appl-id*	Specifies the application ID required when you request an access key from the Azure infrastructure.
directory-id *dir-id*	Specifies the directory ID required when you request an access key from the Azure infrastructure.
key *secret-key*	Specifies the secret key required when you request an access key from the Azure infrastructure. If the **encrypt** keyword is present, the secret key is encrypted in the running configuration.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

To be able to automatically make API calls to modify Azure route tables, the ASA virtual HA units need to have Azure Active Directory credentials. Azure employs the concept of a Service Principal which, in simple terms, is a service account. A Service Proncipal allows you to provision an account with only enough permissions and scope to run a task within a predefined set of Azure resources.

When you have an application that needs to access or modify Azure resources, such as route tables, you must set up an Azure Active Directory (AD) application and assign the required permissions to it.

When you register an Azure AD application in the Azure portal, two objects are created in your Azure AD tenant: an application object, and a service principal object. The service principal object defines the policy and permissions for an application's use in a specific tenant, providing the basis for a security principal to represent the application at run-time.

After you set up the service principal, you obtain the **Directory ID**, **Application ID**, and **Secret key**. Theseare required to configure Azure authentication credentials.

Note Azure provides instructions on how to create an Azure AD application and service principal in the *Azure Resource Manager Documentation* .

Examples

The following example adds the Azure authentication credentials to the public cloud failover configuration:

```
(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-6931704e420
(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138b77ae9
(config)# failover cloud authentication key 5yOhH593dtD/O8gzAlWgulrkWz5dH02d2STk3LDbI4c=
(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.
failover cloud subscription-id	Adds the Azure Subscription ID to the public cloud failover configuration.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover cloud peer

To configure the public cloud failover peer, use the **failover cloud peer** command in global configuration mode. To disable the failover peer, use the **no** form of this command.

failover cloud peer { **ip** *ip-address* | **port** *port-number* }
no failover cloud peer

Syntax Description

ip *ip-address*	Specifies the IP address used to establish a TCP failover control connection to the public cloud HA peer.
port *port-number*	Specifies directory ID required when you request an access key from the Azure infrastructure.

Command Default

The default is the port number specified by the **failover cloud port control** command (or its default if not specified).

Command Modes

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

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

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

The IP address is used to establish a TCP failover control connection to the public cloud HA peer. The port is used when attempting to open a failover connection to the HA peer, who may already by the Active unit. Configuring the port here may be needed if NAT is being performed between the HA peers. In most cases it won't need to be configured.

The **no** version of this command removes the peer IP address and sets the port number to its default value. If the port is not specified, the port number is set to its default value, even it is was set to a different value previously using this command.

Examples

The following example configures a public cloud failover peer:

```
ciscoasa(config)# failover cloud peer ip 10.4.3.5 port 4444
ciscoasa(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 cloud polltime

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

failover cloud polltime *poll_time* [**holdtime** *time*]
no failover cloud polltime

Syntax Description

holdtime *time*	(Optional) Sets the time during which a unit must receive a hello message on the control port, after which the peer unit is declared failed. Valid values are from 3 to 60 seconds. You cannot enter a holdtime value that is less than 3 times the unit poll time.
polltime *poll_time*	Sets the amount of time between hello messages. Valid values are from 1 to 15 seconds.

Command Default

The default values on the ASA virtual are as follows:

- The **polltime** *poll_time* is 5 second.
- The **holdtime** *time* is 15 seconds.

Command Modes

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

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

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

Used to set the polling interval that the Backup uses for monitoring the presence of the Active unit. Optionally, you can also set the amount of time (hold time) that the Backup unit will wait, in the absence of a response from the Active unit, before taking over the Active role. The hold time will be forced to be at least three times the 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.

Examples

The following example configures failover polling for the public cloud failover configuration:

```
ciscoasa(config)# failover cloud polltime 10 holdtime 30
```

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 cloud port

To specify the two TCP ports used by public cloud failover pairs, the port used for failover communication between the two peers, and the port used for Azure Load Balancer probes, use the **failover cloud port** command in global configuration mode. Use the **no** form of this command restore the default values for these ports.

failover cloud port { **control** *port-number* | **probe** *port-number* [**interface** *if-name*] }
no failover cloud port { **control** | **probe** }

Syntax Description

control *port-number*	(Optional) Specifies the TCP port used to communicate with public cloud HA peer.
probe *port-number*	(Optional) Specifies the TCP port used to respond to Azure Load Balancer health probes.
interface if-name	(Optional) Specifies an interface configured for the probe port which to accept Azure Load Balancer probes. If omitted, probes are accepted on the interface that the IP routing function in the ASA virtual determines is the best for reaching the well-known source IP address used by the probes (168.63.129.16).

Command Default

The public cloud failover TCP control port number is 44442.

The Azure Load Balancer health probe port number is 44441.

Command Modes

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

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

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

Use the **no** form of this command to restore the default port values.

On the physical ASA and the non-public cloud virtual ASA, the system handles failover conditions using gratuitous ARP requests where the backup ASA sends out a gratuitous ARP indicating it is now associated with the active IP and MAC addresses. Most public cloud environments do not allow broadcast traffic of this nature. For this reason, an HA configuration in the public cloud requires ongoing connections be restarted when failover happens.

The health of the active unit is monitored by the backup unit to determine if specific failover conditions are met. If those conditions are met, failover occurs. The failover time can vary from a few seconds to over a minute depending on the responsiveness of the public cloud infrastructure.

Examples

The following example configures TCP ports for failover communication and Azure Load Balancer probes to the public cloud failover configuration:

```
ciscoasa(config)# failover cloud port control 4444
ciscoasa(config)# failover cloud port probe 4443
```

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 cloud route-table

To configure an Azure route table that directs internal routes to the Active unit, use the **failover cloud route-table** command in global configuration mode. To remove the route table configuration, use the **no** form of this command.

failover cloud route-table table-name [**subscription-id** *sub-id*]
no failover cloud route-table

Syntax Description

table-name	Specifies the name of the route table.
subscription-id *sub-id*	(Optional) Specifies the Azure Subscription ID, required when you want to modify Azure resources. If this parameter is present for a route table, this is the Azure subscription used when referencing the route table. If omitted, the subscription ID configured in global configuration mode is used.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
9.8(2)	This command was introduced.
9.9(2)	The **subscription-id** parameter was introduced.

Usage Guidelines

On failover, you want to direct internal routes to the active unit, which uses the configured route table information to automatically direct the routes to itself.

Configure these settings on both the primary and secondary units. There is no synching of configuration from the primary unit to the secondary unit.

To update user-defined routes in more than one Azure subscription, use the optional **subscription-id** parameter. The **subscription-id** at the **route-table** command level overrides the Azure Subscription ID specified at the global level. If you enter the **route-table** command without specifying the **subscription-id**, the global parameter is used.

Use the **no** form of this command remove the route table configuration.

Note When you enter this command the ASA virtual switches to **cfg-fover-cloud-rt** mode.

Examples

The following examples show how to enable the cfg-fover-cloud-rt mode for public cloud failover route table configuration:

```
ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)#
ciscoasa(config)# failover cloud route-table inside-rt subscription-id cd5fe6b4-d2ed-45
ciscoasa(cfg-fover-cloud-rt)#
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
rg	Adds an Azure resource group to the public cloud failover configuration.
route-table	Adds Azure route information to the public cloud failover configuration.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.
failover cloud subscription-id	Adds the Azure Subscription ID to the public cloud failover configuration.

failover cloud route-table rg

To configure an Azure resource group, required for route table update requests, use the **rg** command in cfg-fover-cloud-rt configuration mode. To remove the resource group information from the configuration, use the **no** form of this command.

rg*resource-group*
no rg

Syntax Description

resource-group	Specifies the name of the Azure resource group.

Command Default

No default behaviors or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
cfg-fover-cloud-rt configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

An Azure resource group is a container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization.

Configure these settings on both the primary and secondary units. There is no synching of configuration from the primary unit to the secondary unit.

Use the **no** form of this command remove the resource group information from the configuration.

Note Azure provides information about resource groups in the *Azure Resource Manager Documentation* .

Examples

The following example adds an Azure resource group to the public cloud failover configuration:

```
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)#
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
rg	Adds an Azure resource group to the public cloud failover configuration.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover cloud route-table route

To configure an route that requires updating during a failover, use the **route** command in cfg-fover-cloud-rt configuration mode. To remove the route information from the configuration, use the **no** form of this command.

route { **name** *route-name* **prefix** *address-prefix* **nexthop** *ip-address* }
no route name *route-name*

Syntax Description

route-name	Specifies the name of the route.
address-prefix	Specifies the address prefix, configured as an IP address prefix, a slash ('/') and a numerical netmask. For example '192.120.0.0/16'.
ip-address	Specifies the next hop IP address.

Command Default

No default behaviors or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
cfg-fover-cloud-rt configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

On failover, you want to direct internal routes to the active unit, which uses the configured route table information to automatically direct the routes to itself.

Configure these settings on both the primary and secondary units. There is no synching of configuration from the primary unit to the secondary unit.

Use the **no** form of this command remove the route information from the configuration.

Note Azure provides information about routing requirements in the *Azure Resource Manager Documentation* .

Examples

The following example adds a route that requires updating to the public cloud failover configuration:

```
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4
ciscoasa(cfg-fover-cloud-rt)#
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
rg	Adds an Azure resource group to the public cloud failover configuration.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover cloud subscription-id

To configure the Azure Subscription ID for the Azure Service Principal, use the **failover cloud subscription-id** command in global configuration mode. The **no** form of this command removes the subscription information from the configuration.

failover cloud subscription-id *sub-id*
no failover cloud subscription-id

Syntax Description

subscription-id *sub-id*	Specifies your Azure Subscription ID, required when you want to modify Azure resources.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

The Azure Subscription ID is needed to modify Azure route tables, for example, when you want to direct internal routes to the active unit.

Note You should be able to find your Subscription ID from the ‘Subscriptions’ tab of the Azure Portal, https://portal.azure.com .

Examples

The following example adds the Azure subscription ID to the public cloud failover configuration:

```
(config)# failover cloud (config)# failover cloud subscription-id ab2fe6b2-c2bd-44
(config)#
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.

Command	Description
failover cloud authentication	Adds the Azure authentication credentials to the public cloud failover configuration.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover cloud unit

To configure the ASA virtual as either the primary or secondary unit in a public cloud failover configuration, use the **failover lan unit** command in global configuration mode. To remove the unit role setting, use the **no** form of this command.

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

Syntax Description

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

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
9.8(2)	This command was introduced.

Usage Guidelines

To ensure redundancy, you can deploy the ASA virtual in a public cloud environment in an Active/Backup high availability (HA) configuration. HA in the public cloud implements a stateless Active/Backup solution that allows for a failure of the active ASA virtual to trigger an automatic failover of the system to the backup ASA virtual.

When setting up Active/Backup failover, you configure one unit to be primary and the other as secondary. At this point, the two units act as two separate devices for device and policy configuration, as well as for events, dashboards, reports and health monitoring.

The main differences between the two units in a failover pair are related to which unit is active and which unit is backup, namely which unit actively passes traffic. Although both units are capable of passing traffic, only the primary unit responds Load Balancer probes and programs any configured routes to use it as a route destination. The backup unit's primary function is to monitor the health of the primary unit. The primary unit always becomes the active unit if both units start up at the same time (and are of equal operational health).

Examples

The following example sets the ASA virtual as the primary unit in a public cloud failover configuration:

```
ciscoasa(config)# failover cloud unit primary
```

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.
failover cloud peer	Specifies public cloud failover peer information.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

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.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

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:

```
ciscoasa(config)# failover exec interface GigabitEthernet0/1
ciscoasa(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:

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

```
ciscoasa(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
ciscoasa(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.

```
ciscoasa(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.

```
ciscoasa(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.

```
ciscoasa(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.
ciscoasa(config)# failover exec active context text
```

```
Creating context 'text'... Done. (2)
Creating context 'text'... Done. (3)
ciscoasa(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:

```
ciscoasa# 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.
ciscoasa(config)#
```

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

```
ciscoasa(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:

```
ciscoasa# 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:

```
ciscoasa(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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(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 health-check bfd

To configure Bidirectional Forwarding Detection (BFD) for unit health monitoring, use the **failover health-check bfd** command in global configuration mode. To disable BFD, use the **no** form of this command.

failover health-check bfd *template_name*
no failover health-check bfd *template_name*

Syntax Description

template_name	The name of a BFD template.

Command Default

This command is disabled by default.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.7(1)	We introduced this command.

Usage Guidelines

The regular unit monitoring can cause false alarms when CPU usage is high. The BFD method is distributed, so high CPU does not affect its operation.

You must first configure a BFD single-hop template to define the packet rate:

bfd-template single-hop *template_name*

bfd interval min-tx *milliseconds* **min-rx** *milliseconds* **multiplier** *multiplier_value*

See the following limitations:

- Firepower 9300 and 4100 only.
- Active/Standby only.
- Routed mode only

Examples

The following example enables BFD unit health detection:

```
ciscoasa(config)# bfd template single-hop failover-temp
ciscoasa(config-bfd)# bfd interval min-tx 50 min-rx 50 multiplier 3
ciscoasa(config)# failover health-check bfd failover-temp
```

Related Commands

Command	Description
bfd template	Creates a template for use with BFD.
bfd interval	Defines the packet rate for the template.

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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

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

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:

```
ciscoasa(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:

```
ciscoasa(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.

Command Default

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:

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa(config)# failover interface-policy 20%
ciscoasa(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:

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

Command History

Release	Modification
9.1(2)	This command was added.

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 If you configure HA failover encryption in evaluation mode, the systems use DES for the encryption. If you then register the devices using an export-compliant account, the devices will use AES after a reboot. Thus, if a system reboots for any reason, including after installing an upgrade, the peers will be unable to communicate and both units will become the active unit. We recommend that you do not configure encryption until after you register the devices. If you do configure this in evaluation mode, we recommend you remove the encryption before registering the devices.

When you use this command, the system creates an IKE policy. Because the system allows a maximum of 20 IKE policies, if there are already 20, this command will fail.

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:

```
ciscoasa(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.

Command Default

0 (unencrypted) is the default.

Command Modes

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

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

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.

Note If you configure HA failover encryption in evaluation mode, the systems use DES for the encryption. If you then register the devices using an export-compliant account, the devices will use AES after a reboot. Thus, if a system reboots for any reason, including after installing an upgrade, the peers will be unable to communicate and both units will become the active unit. We recommend that you do not configure encryption until after you register the devices. If you do configure this in evaluation mode, we recommend you remove the encryption before registering the devices.

Examples

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

```
ciscoasa(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:

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

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

```
ciscoasa(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 ASASM to specify a VLAN interface as the failover link.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The *phy_if* argument was added.
7.2(1)	The *vlan_if* argument was added.
9.5(1)	This command was modified to accept the management interface on the ASA 5506H-X.

Usage Guidelines

Do not use this command when both primary and secondary units have failover enabled. Changing the failover interface configuration leads to a split-brain scenario (Active-Active).

The two units in a failover pair constantly communicate over a failover link to determine the operating status of each unit.

Failover Link Data

The following information is communicated over the failover link:

- The unit state (active or standby)
- Hello messages (keep-alives)

- Network link status
- MAC address exchange
- Configuration replication and synchronization

Interface for the Failover Link

You can use any unused data interface (physical, redundant, or EtherChannel) as the failover link; however, you cannot specify an interface that is currently configured with a name. The failover link interface is not configured as a normal networking interface; it exists for failover communication only. This interface can only be used for the failover link (and also for the state link). The ASA does not support sharing interfaces between user data and the failover link even if different subinterfaces are configured for user data and failover. A separate physical, EtherChannel, or redundant interface must be used for the failover link.

See the following guidelines for the failover link:

- 5506-X through 5555-X—You cannot use the Management interface as the failover link; you must use a data interface. The only exception is for the 5506H-X, where you can use the management interface as the failover link.
- 5506H-X—You can use the Management 1/1 interface as the failover link. If you configure it for failover, you must reload the device for the change to take effect. In this case, you cannot also use the ASA Firepower module, because it requires the Management interface for management purposes.
- 5585-X—Do not use the Management 0/0 interface, even though it can be used as a data interface. It does not support the necessary performance for this use.
- Firepower 9300 ASA security module—You can use either a management type or data type interface as the failover link. To conserve interfaces and to share a failover link between modules in the same chassis, use a management type interface. For example, you have 2 chassis, each with 3 ASA security modules. You can create 3 failover pairs between the chassis. You can use a single 10 GigabitEthernet management interface between the chassis to act as the failover link. Just configure a unique VLAN subinterface within each module.
- All models—1 GB interface is large enough for a combined failover and state link.

For a redundant interface used as the failover link, see the following benefits for added redundancy:

- When a failover unit boots up, it alternates between the member interfaces to detect an active unit.
- If a failover unit stops receiving keepalive messages from its peer on one of the member interfaces, it switches to the other member interface.

For an EtherChannel used as the failover link, to prevent out-of-order packets, only one interface in the EtherChannel is used. If that interface fails, then the next interface in the EtherChannel is used. You cannot alter the EtherChannel configuration while it is in use as a failover link.

Connecting the Failover Link

Connect the failover link in one of the following two ways:

- Using a switch, with no other device on the same network segment (broadcast domain or VLAN) as the failover interfaces of the ASA.
- Using an Ethernet cable to connect the units directly, without the need for an external switch.

If you do not use a switch between the units, if the interface fails, the link is brought down on both peers. This condition may hamper troubleshooting efforts because you cannot easily determine which unit has the failed interface and caused the link to come down.

The ASA supports Auto-MDI/MDIX on its copper Ethernet ports, so you can either use a crossover cable or a straight-through cable. If you use a straight-through cable, the interface automatically detects the cable and swaps one of the transmit/receive pairs to MDIX.

Additional Guidelines

- When using VLANs on connecting switches, 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.
- The IP address and MAC address for the failover link do not change at 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 parameters for the primary unit, including a shared failover and state link:

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
interface gigabitethernet 0/3
no shutdown
failover link folink gigabitethernet0/3
failover ipsec pre-shared-key a3rynsun
failover
```

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.

Command Default

Secondary.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa(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 and to enable Stateful Failover, 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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The *phy_if* argument was added.
7.0(4)	This command was modified to accept standard firewall interfaces.
9.5(1)	This command was modified to accept the management interface on the ASA 5506H-X.

Usage Guidelines

To use Stateful Failover, you must configure a Stateful Failover link (also known as the state link) to pass connection state information.

Shared with the Failover Link

Sharing a failover link is the best way to conserve interfaces. If you experience performance problems on that interface, consider dedicating a separate interface for the state link.

Dedicated Interface

You can use a dedicated data interface (physical, redundant, or EtherChannel) for the state link. For an EtherChannel used as the state link, to prevent out-of-order packets, only one interface in the EtherChannel is used. If that interface fails, then the next interface in the EtherChannel is used.

Connect a dedicated state link in one of the following two ways:

- Using a switch, with no other device on the same network segment (broadcast domain or VLAN) as the failover interfaces of the ASA.
- Using an Ethernet cable to connect the appliances directly, without the need for an external switch.

If you do not use a switch between the units, if the interface fails, the link is brought down on both peers. This condition may hamper troubleshooting efforts because you cannot easily determine which unit has the failed interface and caused the link to come down.

The ASA supports Auto-MDI/MDIX on its copper Ethernet ports, so you can either use a crossover cable or a straight-through cable. If you use a straight-through cable, the interface automatically detects the cable and swaps one of the transmit/receive pairs to MDIX.

For optimum performance when using long distance failover, the latency for the state link should be less than 10 milliseconds and no more than 250 milliseconds. If latency is more than10 milliseconds, some performance degradation occurs due to retransmission of failover messages.

Additional Guidelines

- 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.
- 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 configures the failover parameters for the primary unit, including a shared failover and state link:

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
interface gigabitethernet 0/3
no shutdown
failover link folink gigabitethernet0/3
failover ipsec pre-shared-key a3rynsun
failover
```

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.

Command Default

Not configured.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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.

When removing the MAC address using the **no** form of this command, it is recommended to reload both units to ensure the changes 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:

```
ciscoasa(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.

Command Default

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:

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

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.

Release	Modification
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 receive a hello packet on the failover link 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, then 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:

```
ciscoasa(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.

```
ciscoasa(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 polltime and holdtime in an Active/Standby failover configuration, use the **failover polltime interface** command in global configuration mode. To restore the default polltime and holdtime, use the **no** form of this command.

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

Syntax Description

holdtime *time*	(Optional) Sets the time (as a calculation) between the last-received hello message from the peer unit and the commencement of interface tests to determine the health of the interface. It also sets the duration of each interface test as *holdtime* /16. Valid values are from 5 to 75 seconds. The default is 5 times the *polltime* . You cannot enter a holdtime value that is less than five times the *polltime* . To calculate the time before starting interface tests (y): **1.** x = (*holdtime* /*polltime)/2* , rounded to the nearest integer. (.4 and down rounds down; .5 and up rounds up.) **2.** y = x**polltime* For example, if you use the default holdtime of 25 and polltime of 5, then y = 15 seconds.
polltime	Specifies how long to wait between sending a hello packet to the peer. Valid values range from 1 to 15 seconds. The default is 5. 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.

Command Default

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:

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

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

This command is available for Active/Standby failover only. For Active/Active failover, use the **polltime interface** command in failover group configuration mode.

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.

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 polltime frequency to 15 seconds:

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

The following example sets the interface polltime frequency to 500 milliseconds and the holdtime to 5 seconds:

```
ciscoasa(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 poll-time link-state

To change the interface link state poll time, use the **failover polltime link-state** command in global configuration mode. To disable the link-state poll, use the **no** form of this command.

failover polltime link-state msec *poll_time*
no failover polltime link-state msec *poll_time*

Syntax Description

msec *poll_time*	Sets the polltime between 300 and 799 milliseconds.

Command Default

The default polltime is 500 msec.

Command Modes

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

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

Command History

Release	Modification
9.7(1)	We introduced this command.

Usage Guidelines

By default, each ASA in a failover pair checks the link state of its interfaces every 500 msec. You can customize the polltime; for example, if you set the polltime to 300 msec, the ASA can detect an interface failure and trigger failover faster.

In Active/Active mode, you set this rate for the system; you cannot set this rate per failover group.

Examples

The following example sets the link-state polltime to 300 msec:

```
ciscoasa(config)# failover polltime link-state msec 300
```

Related Commands

Command	Description
failover polltime unit	Sets the polltime for the unit health check.
failover polltime interface	Sets the polltime for the interface health check.

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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa# 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.

Command Default

Disabled.

Command Modes

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

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

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.

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:

```
ciscoasa(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:

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

Command History

Release	Modification
8.4(4.1)/8.5(1.7)	This command was added.

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:

```
ciscoasa(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.

Command Default

No default behavior or values.

Command Modes

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

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

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:

```
ciscoasa# 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 standby config-lock

To lock configuration changes on the standby unit or standby context in a failover pair, use the **failover standby config-lock** command in global configuration mode. To allow configuration on the standby unit, use the **no** form of this command.

failover standby config-lock
no failover standby config-lock

Syntax Description

This command has no arguments or keywords.

Command Default

By default, configurations on the standby unit/context are allowed with a warning message.

Command Modes

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

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

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

You can lock configuration changes on the standby unit (Active/Standby failover) or the standby context (Active/Active failover) so you cannot make changes on the standby unit outside normal configuration syncing.

Examples

The following example disallows configuration on the standby unit:

```
ciscoasa(config)# failover standby config-lock
```

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 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**]
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.

Command Default

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:

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

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:

```
ciscoasa(config)# failover timeout 12:30
ciscoasa(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.

failover trace

To configure and view trace levels of a failover trace log, use the **failover trace** command in configuration mode.

failover trace [*options*]

Syntax Description

failover trace [*options*]	(Optional) Shows the failover event trace. Options include to show the failover event trace by levels (1-5): • **critical** — to filter failover critical event trace (level = 1) • **debugging**— to filter failover debugging trace (Debug level = 5) • **error**— to filter failover internal exception (level = 2) • **informational**— to filter failover informational trace (level = 4) • **warning**— to filter failover warnings (level = 3)

Command Default

Default value is configurable only in version 9.16.

Command Modes

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

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

Command History

Release	Modification
9.16	This command is available only in version 9.16.
9.18	This command is no longer configurable and set to informational by default.

Usage Guidelines

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

failover wait-disable

When using bridge groups or IPv6 duplicate address detection (DAD), to disable waiting for the failover peer unit to go into the standby state, use the **failover wait-disable** command in global configuration mode. With these features, the new active unit waits to pass traffic until after the standby unit finishes network tasks and transitions to the standby state. To reenable waiting, use the **no** form of this command.

failover wait-disable
no failover wait-disable

Command Default

By default, the active unit will wait up to 3000 ms for the standby unit to finish transitiong to the standby state (**no failover wait-disable**).

Command Modes

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

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

Command History

Release	Modification
9.15(1)	This command was introduced.

Usage Guidelines

When you use bridge groups or IPv6 DAD, when a failover occurs the new active unit waits up to 3000 ms for the standby unit to finish networking tasks and transition to the standby state. Then the active unit can start passing traffic. To avoid this delay, you can disable the waiting time, and the active unit will start passing traffic before the standby unit transitions.

Examples

The following example disables waiting:

```
ciscoasa(config)# failover wait-disable
ciscoasa(config)#
```

fallback (Deprecated)

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 { **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.

Command Default

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

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

Command History

Release	Modification
8.3(1)	The command was added.
9.4(1)	This command was deprecated along with all **uc-ime** mode commands.

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:

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

```
ciscoasa
(config)# uc-ime local_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(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.

fast-flood

To fill IS-IS link-state packets (LSPs), use the **fast-flood** command in router isis configuration mode. To disable the fast flooding, use the **no** form of this command.

fast-flood [*lsp-number*]
no fast-flood [*lsp-number*]

Syntax Description

lsp-number	(Optional) The number of LSPs to be flooded before the SPF is started. The range is 1 to 15. The default is 5.

Command Default

Fast flooding is disabled.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	The command was added.

Usage Guidelines

The **fast-flood** command sends a specified number of LSPs from the ASA. If no LSP number value is specified, the default it 5. The LSPs invoke SPF before running SPF. When you speed up the LSP flooding process, you improve overall network convergence time.

The ASA should always flood, at least, the LSP that triggered SPF before the router runs the SPF computation.

We recommend that you enable the fast flooding of LSPs before the ASA runs the SPF computation, in order to achieve a faster convergence time

Examples

In the following example, the **fast-flood** command is entered to configure the ASA to fill the first seven LSPs that invoke SPF, before the SPF computation is started. When the **show running-configuration** command is entered, the output confirms that fast flooding has been enabled on the ASA:

```
ciscoasa# clear isis rib redistribution 10.1.0.0 255.255.0.0
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# router isis
ciscoasa(config-router)# fast-flood 7
ciscoasa(config-router)# end
```

```
ciscoasa# show running-config | inc fast-flood
fast-flood 7
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.

Command	Description
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.

Command	Description
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.