



retries through rtp-min-port rtp-max-port Commands

retries

To specify the number of times to retry the list of DNS servers when the ASA does not receive a response, use the **dns retries** command in global configuration mode. To restore the default setting, use the **no** form of this command.

retries *number*

no retries [*number*]

Syntax Description

number Specifies the number of retries, from 0 through 10. The default is 2.

Defaults

The default number of retries is 2.

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	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Add DNS servers using the **name-server** command.

This command replaces the **dns name-server** command.

Examples

The following example sets the number of retries to 0. The ASA tries each server only once.

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# dns retries 0
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters the dns server-group mode.
show running-config dns server-group	Shows one or all the existing dns-server-group configurations.

retry-count

To set the value for the number of consecutive polling failures to the Cloud Web Security proxy server before determining the server is unreachable, enter the **retry-count** command in scansafe general-options configuration mode. To restore the default, use the **no** form of this command.

retry-count *value*

no retry-count [*value*]

Syntax Description

value Enters the retry counter value, from 2 to 100. The default is 5.

Command Default

The default value is 5.

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
Scansafe general-options configuration	•	•	•	—	•

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

When you subscribe to the Cisco Cloud Web Security service, you are assigned a primary Cloud Web Security proxy server and backup proxy server.

If any client is unable to reach the primary server, then the ASA starts polling the tower to determine availability. (If there is no client activity, the ASA polls every 15 minutes.) If the proxy server is unavailable after a configured number of retries (the default is 5; this setting is configurable), the server is declared unreachable, and the backup proxy server becomes active.

If a client or the ASA can reach the server at least twice consecutively before the retry count is reached, the polling stops and the tower is determined to be reachable.

After a failover to the backup server, the ASA continues to poll the primary server. If the primary server becomes reachable, then the ASA returns to using the primary server.

Examples

The following example configures a retry value of 7:

```
scansafe general-options
server primary ip 180.24.0.62 port 8080
retry-count 7
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
http[s] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {primary backup}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it's the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current http connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

retry-interval

To configure the amount of time between retry attempts for a particular AAA server designated in a previous **aaa-server host** command, use the **retry-interval** command in aaa-server host mode. To reset the retry interval to the default value, use the **no** form of this command.

retry-interval *seconds*

no **retry-interval**

Syntax Description

<i>seconds</i>	Specify the retry interval (1-10 seconds) for the request. This is the time the ASA waits before retrying a connection request.
----------------	---

Defaults

The default retry interval is 10 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
AAA-server host	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was modified to conform to CLI guidelines.

Usage Guidelines

Use the **retry-interval** command to specify or reset the number of seconds the ASA waits between connection attempts. Use the **timeout** command to specify the length of time during which the ASA attempts to make a connection to a AAA server.

Examples

The following examples show the **retry-interval** command in context.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 7
hostname(config-aaa-server-host)# retry-interval 9
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
aaa-server host	Enters aaa-server host configuration mode, so that you can configure AAA server parameters that are host-specific.

clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol
timeout	Specifies the length of time during which the ASA attempts to make a connection to a AAA server.

reval-period

To specify the interval between each successful posture validation in a NAC Framework session, use the **reval-period** command in nac-policy-nac-framework configuration mode. To remove the command from the NAC Framework policy, use the **no** form of this command.

reval-period *seconds*

no reval-period [*seconds*]

Syntax Description

seconds Number of seconds between each successful posture validation. The range is 300 to 86400.

Defaults

The default value is 36000.

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
nac-policy-nac-framework configuration	•	—	•	—	—

Command History

Release	Modification
7.3(0)	“nac-” removed from command name. Command moved from group-policy configuration mode to nac-policy-nac-framework configuration mode.
7.2(1)	This command was introduced.

Usage Guidelines

The ASA starts the revalidation timer after each successful posture validation. The expiration of this timer triggers the next unconditional posture validation. The ASA maintains posture validation during revalidation. The default group policy becomes effective if the Access Control Server is unavailable during posture validation or revalidation.

Examples

The following example changes the revalidation timer to 86400 seconds:

```
hostname(config-nac-policy-nac-framework)# reval-period 86400
hostname(config-nac-policy-nac-framework)
```

The following example removes the revalidation timer from the NAC policy:

```
hostname(config-nac-policy-nac-framework)# no reval-period
hostname(config-nac-policy-nac-framework)
```

Related Commands

Command	Description
eou timeout	Changes the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration.
sq-period	Specifies the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture.
nac-policy	Creates and accesses a Cisco NAC policy, and specifies its type.
debug nac	Enables logging of NAC Framework events.
eou revalidate	Forces immediate posture revalidation of one or more NAC Framework sessions.

revert webvpn all

To remove all web-related data (customization, plug-in, translation table, URL list, and web content) from the ASA flash memory, enter the **revert webvpn all** command in privileged EXEC mode.

revert webvpn all

Defaults

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 mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **revert webvpn all** command to disable and remove all web-related information (customization, plug-in, translation table, URL list, and web content) from the flash memory of the ASA. Removal of all web-related data returns default settings when applicable.

Examples

The following command removes all of the web-related configuration data from the ASA:

```
hostname# revert webvpn all
hostname
```

Related Commands

Command	Description
show import webvpn (<i>option</i>)	Displays various imported WebVPN data and plug-ins. currently present in flash memory on the ASA.

revert webvpn AnyConnect-customization

To remove a file from the ASA that customizes the AnyConnect client GUI, use the **revert webvpn AnyConnect-customization** command in privileged EXEC mode.

revert webvpn AnyConnect-customization *type type platform platform name name*

Syntax Description

<i>type</i>	The type of customizing file: - binary—An executable that replaces the AnyConnect GUI. - resource—A resource file, such as the corporate logo. - transform—A transform that customizes the MSI.
<i>platform</i>	The OS of the endpoint device running the AnyConnect client. Specify one of the following: linux , mac-intel , mac-powerpc , win , or win-mobile .
<i>name</i>	The name that identifies the file to remove (maximum 64 characters).

Defaults

There is no default behavior for this command.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

For detailed procedures for customizing the AnyConnect client GUI, see the *AnyConnect VPN Client Administrator Guide*.

Examples

The following example removes the Cisco logo that was previously imported as a resource file to customize the AnyConnect GUI:

```
hostname# revert webvpn AnyConnect-customization type resource platform win name
cisco_logo.gif
```

Related Commands

Command	Description
<code>customization</code>	Specifies the customization object to use for a tunnel-group, group, or user.
<code>export customization</code>	Exports a customization object.
<code>import customization</code>	Installs a customization object.
<code>revert webvpn all</code>	Removes all webvpn-related data (customization, plug-in, translation table, URL list, and web content).
<code>show webvpn customization</code>	Displays the current customization objects present on the flash device of the ASA.

revert webvpn customization

To remove a customization object from the ASA cache memory, enter the **revert webvpn customization** command in privileged EXEC mode.

revert webvpn customization *name*

Syntax Description

<i>name</i>	Specifies the name of the customization object to be deleted.
-------------	---

Defaults

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 mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **revert webvpn customization** command to remove Clientless SSL VPN support for the specified customization and to remove it from the cache memory on the ASA. Removal of a customization object returns default settings when applicable. A customization object contains the configuration parameters for a specific, named portal page.

Version 8.0 software extends the functionality for configuring customization, and the new process is incompatible with previous versions. During the upgrade to 8.0 software, the security appliance preserves a current configuration by using old settings to generate new customization objects. This process occurs only once, and is more than a simple transformation from the old format to the new one because the old values are only a partial subset of the new ones.



Note

Version 7.2 portal customizations and URL lists work in the Beta 8.0 configuration only if clientless SSL VPN (WebVPN) is enabled on the appropriate interface in the Version 7.2(x) configuration file before you upgrade to Version 8.0.

Examples

The following command removes the customization object named GroupB:

```
hostname# revert webvpn customization groupb
hostname
```

Related Commands

Command	Description
customization	Specifies the customization object to use for a tunnel-group, group, or user.
export customization	Exports a customization object.
import customization	Installs a customization object.
revert webvpn all	Removes all webvpn-related data (customization, plug-in, translation table, URL list, and web content).
show webvpn customization	Displays the current customization objects present on the flash device of the ASA.

revert webvpn plug-in protocol

To remove a plug-in from the flash device of the ASA, enter the **revert webvpn plug-in protocol** command in privileged EXEC mode.

revert plug-in protocol *protocol*

Syntax Description	<i>protocol</i> Enter one of the following strings: • rdp The Remote Desktop Protocol plug-in lets the remote user connect to a computer running Microsoft Terminal Services. • ssh The Secure Shell plug-in lets the remote user establish a secure channel to a remote computer, or lets the remote user use Telnet to connect to a remote computer. • vnc The Virtual Network Computing plug-in lets the remote user use a monitor, keyboard, and mouse to view and control a computer with remote desktop sharing turned on.
--------------------	--

Defaults	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 mode	•	—	•	—	—

Command History	Release	Modification
	8.0(2)	This command was introduced.

Usage Guidelines Use the **revert webvpn plug-in protocol** command to disable and remove Clientless SSL VPN support for the specified Java-based client application, as well as to remove it from the flash drive of the ASA.

Examples

The following command removes support for RDP:

```

hostname# revert webvpn plug-in protocol rdp
hostname

```

Related Commands	Command	Description
	import webvpn plug-in protocol	Copies the specified plug-in from a URL to the flash device of the ASA. Clientless SSL VPN automatically supports the use of the Java-based client application for future sessions when you issue this command.
	show import webvpn plug-in	Lists the plug-ins present on the flash device of the ASA.

revert webvpn translation-table

To remove a translation table from the ASA flash memory, enter the **revert webvpn translation-table** command in privileged EXEC mode.

revert webvpn translation-table *translationdomain language*

Syntax Description

<i>translationdomain</i>	Available translation domains: - AnyConnect - PortForwarder - Banners - CSD - Customization - URL List (Translations of messages from RDP, SSH, and VNC plug-ins.)
<i>language</i>	Specifies the character-encoding method to be deleted.

Defaults

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 mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **revert webvpn translation-table** command to disable and remove an imported translation table and to remove it from the flash memory on the ASA. Removal of a translation table returns default settings when applicable.

Examples

The following command removes the AnyConnect translation table, Dutch:

```
hostname# revert webvpn translation-table anyconnect dutch
hostname
```

Related Commands

Command	Description
revert webvpn all	Removes all webvpn-related data (customization, plug-in, translation table, URL-list, and web content) .
show webvpn translation-table	Displays the current translation tables currently present on the flash device of the ASA.

revert webvpn url-list

To remove a URL list from the ASA, enter the **revert webvpn url-list** command in privileged EXEC mode.

revert webvpn url-list template *name*

Syntax Description

template <i>name</i>	Specifies the name of a URL list.
-----------------------------	-----------------------------------

Defaults

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 mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **revert webvpn url-list** command to disable and remove a current URL list from the flash drive of the ASA. Removal of a url-list returns default settings when applicable.

The template argument used with the **revert webvpn url-list** command specifies the name of a previously configured list of URLs. To configure such a list, use the **url-list** command in global configuration mode.

Examples

The following command removes the URL list, servers2:

```
hostname# revert webvpn url-list servers2
hostname
```

Related Commands

Command	Description
revert webvpn all	Removes all webvpn-related data (customization, plug-in, translation table, URL list, and web content) .
show running-configuration url-list	Displays the current set of configured URL list commands.
url-list (WebVPN mode)	Applies a list of WebVPN servers and URLs to a particular user or group policy.

revert webvpn webcontent

To remove a specified web object from a location in the ASA flash memory, enter the **revert webvpn webcontent** command in privileged EXEC mode.

revert webvpn webcontent *filename*

Syntax Description	<i>filename</i>	Specifies the name of the flash memory file with the web content to be deleted.
---------------------------	-----------------	---

Defaults	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 mode	•	—	•	—	—

Command History	Release	Modification
	8.0(2)	This command was introduced.

Usage Guidelines	Use the revert webvpn content command to disable and remove a file containing the web content and to remove it from the flash memory of the ASA. Removal of web content returns default settings when applicable.
-------------------------	--

Examples	The following command removes the web content file, ABCLogo, from the ASA flash memory:
-----------------	---

```
hostname# revert webvpn webcontent abclogo
hostname
```

Related Commands	Command	Description
	revert webvpn all	Removes all webvpn-related data (customization, plug-in, translation table, URL list, and web content).
	show webvpn webcontent	Displays the web content currently present in flash memory on the ASA.

revocation-check

To define whether revocation checking is needed for the trustpool policy, use the **revocation-check** command in crypto ca trustpool configuration mode. To restore the default revocation checking method, which is *none*, use the **no** form of this command.

revocation-check {[crl] [ocsp] [none] }

no revocation-check {[crl] [ocsp] [none]}

Syntax Description

crl	Specifies that the ASA should use CRL as the revocation checking method.
none	Specifies that the ASA should interpret the certificate status as valid, even if all methods return an error.
ocsp	Specifies that the ASA should use OCSP as the revocation checking method.

Defaults

The default value is *none*.

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
Crypto ca trustpool configuration mode	•	•	•	—	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

The signer of the OCSP response is usually the OCSP server (responder) certificate. After receiving the response, devices try to verify the responder certificate.

Normally a CA sets the lifetime of its OCSP responder certificate to a relatively short period to minimize the chance of compromising its security. The CA includes an ocsf-no-check extension in the responder certificate that indicates it does not need revocation status checking. But if this extension is not present, the device tries to check the certificate revocation status using the revocation methods you configure for the trustpoint with this **revocation-check** command. The OCSP responder certificate must be verifiable if it does not have an ocsf-no-check extension since the OCSP revocation check fails unless you also set the *none* option to ignore the status check.



Note With any permutation of the optional arguments, *none* must be the last keyword used.

The ASA tries the methods in the order in which you configure them, trying the second and third methods only if the previous method returns an error (for example, server down), instead of finding the status as revoked.

You can set a revocation checking method in the client certificate validating trustpoint and also configure no revocation checking (**revocation-check none**) in the responder certificate validating trustpoint. See the **match certificate** command for a configuration example.

If you have configured the ASA with the **revocation-check crl none** command, when a client connects to the ASA, it automatically starts downloading the CRL because it has not been cached, then validates the certificate, and finishes downloading the CRL. In this case, if the CRL is not cached, the ASA validates the certificate before downloading the CRL.

Examples

```
hostname(config-ca-trustpoint)# revocation-check ?

crypto-ca-trustpoint mode commands/options:
  crl    Revocation check by CRL
  none   Ignore revocation check
  ocsf   Revocation check by OCSP
(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpool policy	Enters a submode that provides the commands that define the trustpool policy.
match certificate allow expired-certificate	Allows the administrator to exempt certain certificates from expiration checking.
match certificate skip revocation-check	Allows the administrator to exempt certain certificates from revocation checking.

rewrite

To disable content rewriting a particular application or type of traffic over a WebVPN connection, use the **rewrite** command in webvpn mode. To eliminate a rewrite rule, use the **no** form of this command with the rule number, which uniquely identifies the rule. To eliminate all rewriting rules, use the **no** form of the command without the rule number.

By default, the ASA rewrites, or transforms, all WebVPN traffic.

rewrite order *integer* {**enable** | **disable**} **resource-mask** *string* [**name** *resource name*]

no rewrite order *integer* {**enable** | **disable**} **resource-mask** *string* [**name** *resource name*]

Syntax Description

disable	Defines this rewrite rule as a rule that disables content rewriting for the specified traffic. When you disable content rewriting, traffic does not go through the security appliance.
enable	Defines this rewrite rule as a rule that enables content rewriting for the specified traffic.
<i>integer</i>	Sets the order of the rule among all of the configured rules. The range is 1-65534.
name	(Optional) Identifies the name of the application or resource to which the rule applies.
order	Defines the order in which the ASA applies the rule.
resource-mask	Identifies the application or resource for the rule.
<i>resource name</i>	(Optional) Specifies the application or resource to which the rule applies. Maximum 128 bytes.
<i>string</i>	Specifies the name of the application or resource to match that can contain a regular expression. You can use the following wildcards: Specifies a pattern to match that can contain a regular expression. You can use the following wildcards: * — Matches everything. You cannot use this wildcard by itself. It must accompany an alphanumeric string. ? —Matches any single character. [!seq] — Matches any character not in sequence. [seq] — Matches any character in sequence. Maximum 300 bytes.

Defaults

The default is to rewrite everything.

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
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The ASA performs content rewriting for applications to insure that they render correctly over WebVPN connections. Some applications do not require this processing, such as external public websites. For these applications, you might choose to turn off content rewriting.

You can turn off content rewriting selectively by using the `rewrite` command with the `disable` option to let users browse specific sites directly without going through the ASA. This is similar to split-tunneling in IPsec VPN connections.

You can use this command multiple times. The order in which you configure entries is important because the ASA searches rewrite rules by order number and applies the first rule that matches.

Examples

The following example shows how to configure a rewrite rule, order number of 1, that turns off content rewriting for URLs from `cisco.com` domains:

```
hostname(config-webvpn)# rewrite order 2 disable resource-mask *cisco.com/*
```

Related Commands

Command	Description
apcf	Specifies nonstandard rules to use for a particular application.
proxy-bypass	Configures minimal content rewriting for a particular application.

re-xauth

To require that IPsec users reauthenticate on IKE rekey, issue the **re-xauth enable** command in group-policy configuration mode. To disable user reauthentication on IKE rekey, use the **re-xauth disable** command.

To remove the re-xauth attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value for reauthentication on IKE rekey from another group policy.

re-xauth {enable [extended] | disable}

no re-xauth

Syntax Description

disable	Disables reauthentication on IKE rekey
enable	Enables reauthentication on IKE rekey
extended	Extends the time allowed for reentering authentication credentials until the maximum lifetime of the configured SA.

Defaults

Reauthentication on IKE rekey is disabled.

Command Modes

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

	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
Group policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0.4	The extended keyword was added.

Usage Guidelines

Reauthentication on IKE rekey applies only to IPsec connections.

If you enable reauthentication on IKE rekey, the ASA prompts the user to enter a username and password during initial Phase 1 IKE negotiation and also prompts for user authentication whenever an IKE rekey occurs. Reauthentication provides additional security.

The user has 30 seconds to enter credentials, and up to three attempts before the SA expires at approximately two minutes and the tunnel terminates. Use the **extended** keyword to allow users to reenter authentication credentials until the maximum lifetime of the configured SA.

To check the configured rekey interval, in monitoring mode, issue the **show crypto ipsec sa** command to view the security association lifetime in seconds and lifetime in kilobytes of data.

**Note**

The reauthentication fails if there is no user at the other end of the connection.

Examples

The following example shows how to enable reauthentication on rekey for the group policy named FirstGroup:

```
hostname(config) #group-policy FirstGroup attributes
hostname(config-group-policy) # re-xauth enable
```

rip send version

To specify the RIP version used to send RIP updates on an interface, use the **rip send version** command in interface configuration mode. To restore the defaults, use the **no** form of this command.

```
rip send version {[1] [2]}  
  
no rip send version
```

Syntax Description

1	Specifies RIP Version 1.
2	Specifies RIP Version 2.

Defaults

The ASA sends RIP Version 1 packets.

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
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can override the global RIP send version setting on a per-interface basis by entering the **rip send version** command on an interface.

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Examples

The following example configures the ASA to send and receive RIP Versions 1 and 2 packets on the specified interface:

```
hostname(config)# interface GigabitEthernet0/3  
hostname(config-if)# rip send version 1 2  
hostname(config-if)# rip receive version 1 2
```

Related Commands	Command	Description
	rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.
	router rip	Enables the RIP routing process and enter router configuration mode for that process.
	version	Specifies the version of RIP used globally by the ASA.

rip receive version

To specify the version of RIP accepted on an interface, use the **rip receive version** command in interface configuration mode. To restore the defaults, use the **no** form of this command.

```
version {[1] [2]}

no version
```

Syntax Description	1	Specifies RIP Version 1.
	2	Specifies RIP Version 2.

Defaults The ASA accepts Version 1 and Version 2 packets.

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
Interface configuration	•	—	•	—	—

Command History	Release	Modification
	7.2(1)	This command was introduced.

Usage Guidelines You can override the global setting on a per-interface basis by entering the **rip receive version** command on an interface.

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Examples The following example configures the ASA to receive RIP Versions 1 and 2 packets the specified interface:

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# rip send version 1 2
hostname(config-if)# rip receive version 1 2
```

Related Commands	Command	Description
	rip send version	Specifies the RIP version to use when sending update out of a specific interface.
	router rip	Enables the RIP routing process and enter router configuration mode for that process.
	version	Specifies the version of RIP used globally by the ASA.

rip authentication mode

To specify the type of authentication used in RIP Version 2 packets, use the **rip authentication mode** command in interface configuration mode. To restore the default authentication method, use the **no** form of this command.

rip authentication mode {text | md5}

no rip authentication mode

Syntax Description

md5	Uses MD5 for RIP message authentication.
text	Uses clear text for RIP message authentication (not recommended).

Defaults

Clear text authentication is used 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
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Use the **show interface** command to view the **rip authentication** commands on an interface.

Examples

The following examples shows RIP authentication configured on interface GigabitEthernet0/3:

```
hostname(config)# interface Gigabit0/3
hostname(config-if)# rip authentication mode md5
hostname(config-if)# rip authentication key thisismykey key_id 5
```

Related Commands

Command	Description
rip authentication key	Enables RIP Version 2 authentication and specifies the authentication key.
rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.

Command	Description
rip send version	Specifies the RIP version to use when sending update out of a specific interface.
show running-config interface	Displays the configuration commands for the specified interface.
version	Specifies the version of RIP used globally by the ASA.

rip authentication key

To enable authentication of RIP Version 2 packets and specify the authentication key, use the **rip authentication key** command in interface configuration mode. To disable RIP Version 2 authentication, use the **no** form of this command.

rip authentication key [**0** | **8**] *string* **key_id** *id*

no rip authentication key

Syntax Description

0	Specifies an unencrypted password will follow.
8	Specifies an encrypted password will follow.
<i>id</i>	Specifies the key identification value; valid values range from 1 to 255.
key	Specifies the shared key to be used for the authentication key string. The key can contain up to 16 characters.
<i>string</i>	Specifies the unencrypted (cleartext) user password.

Defaults

RIP authentication 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
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates. When you enable neighbor authentication, you must ensure that the *key* and *key_id* arguments are the same as those used by neighbor devices that provide RIP version 2 updates. The *key* is a text string of up to 16 characters.

Use the **show interface** command to view the **rip authentication** commands on an interface.

Examples

The following examples shows RIP authentication configured on interface GigabitEthernet0/3:

```
hostname(config)# interface Gigabit0/3
hostname(config-if)# rip authentication mode md5
hostname(config-if)# rip authentication key 8 yWlvi0qJAnGK5MRWQzrhIohkGP1wKb 5
```

Related Commands

Command	Description
rip authentication mode	Specifies the type of authentication used in RIP Version 2 packets.
rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.
rip send version	Specifies the RIP version to use when sending update out of a specific interface.
show running-config interface	Displays the configuration commands for the specified interface.
version	Specifies the version of RIP used globally by the ASA.

rip receive version

To specify the version of RIP accepted on an interface, use the **rip receive version** command in interface configuration mode. To restore the defaults, use the **no** form of this command.

```
version {[1] [2]}

no version
```

Syntax Description

1	Specifies RIP Version 1.
2	Specifies RIP Version 2.

Defaults

The ASA accepts Version 1 and Version 2 packets.

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
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can override the global setting on a per-interface basis by entering the **rip receive version** command on an interface.

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Examples

The following example configures the ASA to receive RIP Versions 1 and 2 packets the specified interface:

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# rip send version 1 2
hostname(config-if)# rip receive version 1 2
```

Related Commands	Command	Description
	rip send version	Specifies the RIP version to use when sending update out of a specific interface.
	router rip	Enables the RIP routing process and enters router configuration mode for that process.
	version	Specifies the version of RIP used globally by the ASA.

rip send version

To specify the RIP version used to send RIP updates on an interface, use the **rip send version** command in interface configuration mode. To restore the defaults, use the **no** form of this command.

```
rip send version {[1] [2]}  
  
no rip send version
```

Syntax Description	1	Specifies RIP Version 1.
	2	Specifies RIP Version 2.

Defaults The ASA sends RIP Version 1 packets.

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
Interface configuration	•	—	•	—	—

Command History	Release	Modification
	7.2(1)	This command was introduced.

Usage Guidelines You can override the global RIP send version setting on a per-interface basis by entering the **rip send version** command on an interface.

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Examples The following example configures the ASA to send and receive RIP Versions 1 and 2 packets on the specified interface:

```
hostname(config)# interface GigabitEthernet0/3  
hostname(config-if)# rip send version 1 2  
hostname(config-if)# rip receive version 1 2
```

Related Commands

Command	Description
rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.
router rip	Enables the RIP routing process and enter router configuration mode for that process.
version	Specifies the version of RIP used globally by the ASA.

rmdir

To remove the existing directory, use the **rmdir** command in privileged EXEC mode.

rmdir [/noconfirm] [disk0: | disk1: | flash:]*path*

Syntax Description	/noconfirm	(Optional) Suppresses the confirmation prompt.
	disk0:	(Optional) Specifies the nonremovable internal flash memory, followed by a colon.
	disk1:	(Optional) Specifies the removable external flash memory card, followed by a colon.
	flash:	(Optional) Specifies the nonremovable internal flash, followed by a colon. In the ASA 5500 series adaptive security appliances, the flash keyword is aliased to disk0 .
	<i>path</i>	(Optional) The absolute or relative path of the directory to remove.

Defaults 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	•	•	•	—	•

Command History	Release	Modification
	7.0(1)	This command was introduced.

Usage Guidelines If the directory is not empty, the **rmdir** command fails.

Examples The following example shows how to remove an existing directory named “test”:

```
hostname# rmdir test
```

Related Commands	Command	Description
	dir	Displays the directory contents.
	mkdir	Creates a new directory.
	pwd	Displays the current working directory.
	show file	Displays information about the file system.

route

To enter a static or default route for the specified interface, use the **route** command in global configuration mode. To remove routes from the specified interface, use the **no** form of this command.

route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track number**] | **tunneled**]

no route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track number**] | **tunneled**]

Syntax Description

<i>gateway_ip</i>	Specifies the IP address of the gateway router (the next-hop address for this route).
	Note The <i>gateway_ip</i> argument is optional in transparent mode.
<i>interface_name</i>	Specifies the internal or external network interface name through which the traffic is routed.
<i>ip_address</i>	Specifies the internal or external network IP address.
<i>metric</i>	(Optional) Specifies the administrative distance for this route. Valid values range from 1 to 255. The default value is 1.
<i>netmask</i>	Specifies a network mask to apply to <i>ip_address</i> .
track number	(Optional) Associates a tracking entry with this route. Valid values are from 1 to 500.
	Note The track option is only available in single, routed mode.
tunneled	Specifies the route as the default tunnel gateway for VPN traffic.

Defaults

The *metric* default is 1.

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	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	The track number value was added.

Usage Guidelines

Use the **route** command to enter a default or static route for an interface. To enter a default route, set *ip_address* and *netmask* to **0.0.0.0**, or use the shortened form of **0**. All routes that are entered using the **route** command are stored in the configuration when it is saved.

You can define a separate default route for tunneled traffic along with the standard default route. When you create a default route with the **tunneled** option, all traffic from a tunnel terminating on the ASA that cannot be routed using learned or static routes, is sent to this route. For traffic emerging from a tunnel, this route overrides over any other configured or learned default routes.

The following restrictions apply to default routes with the **tunneled** option:

- Do not enable unicast RPF (**ip verify reverse-path**) on the egress interface of a tunneled route. Enabling uRPF on the egress interface of a tunneled route causes the session to fail.
- Do not enable TCP intercept on the egress interface of the tunneled route, because the session will fail.
- Do not use the VoIP inspection engines (CTIQBE, H.323, GTP, MGCP, RTSP, SIP, SKINNY), the DNS inspect engine, or the DCE RPC inspection engine with tunneled routes. These inspection engines ignore the tunneled route.

You cannot define more than one default route with the **tunneled** option; ECMP for tunneled traffic is not supported.

Create static routes to access networks that are connected outside a router on any interface. For example, the ASA sends all packets that are destined to the 192.168.42.0 network through the 192.168.1.5 router with the following static **route** command.

```
hostname(config)# route dmz 192.168.42.0 255.255.255.0 192.168.1.5 1
```

After you enter the IP address for each interface, the ASA creates a CONNECT route in the route table. This entry is not deleted when you use the **clear route** or **clear configure route** commands.

If the **route** command uses the IP address from one of the interfaces on the ASA as the gateway IP address, the ASA will ARP for the destination IP address in the packet instead of ARPing for the gateway IP address.

Examples

The following example shows how to specify one default **route** command for an outside interface:

```
hostname(config)# route outside 0 0 209.165.201.1 1
```

The following example shows how to add these static **route** commands to provide access to the networks:

```
hostname(config)# route dmz1 10.1.2.0 255.0.0.0 10.1.1.4 1
hostname(config)# route dmz1 10.1.3.0 255.0.0.0 10.1.1.4 1
```

The following example uses an SLA operation to install a default route to the 10.1.1.1 gateway on the outside interface. The SLA operation monitors the availability of that gateway. If the SLA operation fails, then the backup route on the DMZ interface is used.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# route outside 0.0.0.0 0.0.0.0 10.1.1.1 track 1
hostname(config)# route dmz 0.0.0.0 0.0.0.0 10.2.1.1 254
```

Related Commands	Command	Description
	clear configure route	Removes statically configured route commands.
	clear route	Removes routes learned through dynamic routing protocols such as RIP.
	show route	Displays route information.
	show running-config route	Displays configured routes.

route-map

To define the conditions for redistributing routes from one routing protocol into another, use the **route-map** command in global configuration mode. To remove a map, use the **no** form of this command.

```
route-map map_tag [permit | deny] [seq_num]

no route-map map_tag [permit | deny] [seq_num]
```

Syntax Description

deny	(Optional) Specifies that if the match criteria are met for the route map, the route is not redistributed.
map_tag	Text for the route map tag; the text can be up to 57 characters in length.
permit	(Optional) Specifies that if the match criteria is met for this route map, the route is redistributed as controlled by the set actions.
seq_num	(Optional) Route map sequence number; valid values are from 0 to 65535. Indicates the position that a new route map will have in the list of route maps already configured with the same name.

Defaults

- The defaults are as follows:
- **permit.**
 - If you do not specify a *seq_num*, a *seq_num* of 10 is assigned to the first route map.

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	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

The **route-map** command lets you redistribute routes.

The **route-map** global configuration command and the **match** and **set** configuration commands define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria that are the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions, which are the redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match route-map** configuration command has multiple formats. You can enter the **match** commands in any order, and all **match** commands must pass to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** form of the **match** commands removes the specified match criteria.

Use route maps when you want detailed control over how routes are redistributed between routing processes. You specify the destination routing protocol with the **router ospf** global configuration command. You specify the source routing protocol with the **redistribute** router configuration command.

When you pass routes through a route map, a route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command is ignored; the route is not advertised for outbound route maps and is not accepted for inbound route maps. To modify only some data, you must configure a second route map section with an explicit match specified.

The *seq_number* argument is as follows:

1. If you do not define an entry with the supplied tag, an entry is created with the *seq_number* argument set to 10.
2. If you define only one entry with the supplied tag, that entry becomes the default entry for the following **route-map** command. The *seq_number* argument of this entry is unchanged.
3. If you define more than one entry with the supplied tag, an error message is printed to indicate that the *seq_number* argument is required.

If the **no route-map map-tag** command is specified (with no *seq-num* argument), the whole route map is deleted (all **route-map** entries with the same *map-tag* text).

If the match criteria are not met, and you specify the **permit** keyword, the next route map with the same *map_tag* is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.

Examples

The following example shows how to configure a route map in OSPF routing:

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# show running-config route-map
route-map maptag1 permit 8
    set metric 5
    match metric 5
hostname(config-route-map)# exit
hostname(config)#
```

Related Commands

Command	Description
clear configure route-map	Removes the conditions for redistributing the routes from one routing protocol into another routing protocol.
match interface	Distributes distribute any routes that have their next hop out one of the interfaces specified,
router ospf	Starts and configures an OSPF routing process.
set metric	Specifies the metric value in the destination routing protocol for a route map.
show running-config route-map	Displays the information about the route map configuration.

router-alert

To define an action when the Router Alert IP option occurs in a packet with IP Options inspection, use the **router-alert** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

```
router-alert action {allow | clear}

no router-alert action {allow | clear}
```

Syntax Description	allow	Instructs the ASA to allow a packet containing the Router Alert IP option to pass.
	clear	Instructs the ASA to clear the Router Alert IP option from a packet and then allow the packet to pass.

Defaults By default, IP Options inspection, drops packets containing the Router Alert IP option.

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
Parameters configuration	•	•	•	•	—

Command History	Release	Modification
	8.2(2)	This command was introduced.

Usage Guidelines This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. Configuring this inspection instructs the ASA to allow a packet to pass or to clear the specified IP options and then allow the packet to pass.

The Router Alert (RTRALT) or IP Option 20 notifies transit routers to inspect the contents of the packet even when the packet is not destined for that router. This inspection is valuable when implementing RSVP and similar protocols require relatively complex processing from the routers along the packets delivery path.

Examples The following example shows how to set up an action for protocol violation in a policy map:

```
hostname(config)# policy-map type inspect ip-options ip-options_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# eool action allow
hostname(config-pmap-p)# nop action allow
```

```
hostname(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

router-id

To use a fixed router ID, use the **router-id** command in router configuration mode for OSPFv2 or IPv6 router configuration mode for OSPFv3. To reset OSPF to use the previous router ID behavior, use the **no** form of this command.

router-id *id*

no router-id [*id*]

Syntax Description

<i>id</i>	Specifies the router ID in IP address format.
-----------	---

Defaults

If not specified, the highest-level IP address on the ASA is used as the router ID.

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 configuration	•	—	•	•	—
IPv6 router configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0(2)	The processing order for this command was changed. The command is now processed before the network commands in an OSPFv2 configuration.
9.0(1)	Multiple context mode and OSPFv3 are supported.

Usage Guidelines

By default, the ASA uses the highest-level IP address on an interface that is covered by a **network** command in the OSPF configuration. If the highest-level IP address is a private address, then that address is sent in hello packets and database definitions. To use a specific router ID, use the **router-id** command to specify a global address for the router ID.

Router IDs must be unique within an OSPF routing domain. If two routers in the same OSPF domain are using the same router ID, routing may not work correctly.

You should enter the **router-id** command before entering **network** commands in an OSPF configuration. This prevents possible conflicts with the default router ID generated by the ASA. If you do have a conflict, you will receive the message:

```
ERROR: router-id id in use by ospf process pid
```

To enter the conflicting ID, remove the **network** command that contains the IP address causing the conflict, enter the **router-id** command, and then re-enter the **network** command.

Clustering

In Layer 2 clustering, you either need to configure the **router-id id** command or leave the router ID blank, provided all units receive the same router ID.

Examples

The following example sets the router ID to 192.168.1.1:

```
hostname(config-rtr) # router-id 192.168.1.1  
hostname(config-rtr) #
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPFv2 routing processes.

router-id cluster-pool

To specify the router ID cluster pool for a Layer 3 clustering deployment, use the **router-id cluster-pool** command in router configuration mode for OSPFv2 or IPv6 router configuration mode for OSPFv3.

router-id cluster-pool *hostname* | **A.B.C.D** *ip_pool*

Syntax Description

cluster-pool	Enables configuration of an IP address pool when Layer 3 clustering is configured.
hostname A.B.C.D	Specifies the OSPF router ID for this OSPF process.
<i>ip_pool</i>	Specifies the name of the IP address pool.

Defaults

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
Router configuration	•	—	•	—	—
IPv6 router configuration	•	—	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

Router IDs must be unique within an OSPFv2 or OSPFv3 routing domain in clustering. If two routers in the same OSPFv2 or OSPFv3 domain are using the same router ID, routing in clustering may not work correctly.

In Layer 2 clustering, you either need to configure the **router-id id** command or leave the router ID blank, provided all units receive the same router ID.

When a Layer 3 cluster interface is configured, each unit must have a unique interface IP address. To make sure that each unit has a unique interface IP address, you can configure a local pool of IP addresses for OSPFv2 or OSPFv3 with the **router-id cluster-pool** command.

Examples

The following example shows how to configure an IP address pool when Layer 3 clustering is configured for OSPFv2:

```
hostname(config)# ip local pool rpool 1.1.1.1-1.1.1.4
hostname(config)# router ospf 1
hostname(config-rtr)# router-id cluster-pool rpool
hostname(config-rtr)# network 17.5.0.0 255.255.0.0 area 1
```

```
hostname(config-rtr)# log-adj-changes
```

The following example shows how to configure an IP address pool when Layer 3 clustering is configured for OSPFv3:

```
hostname(config)# ipv6 router ospf 2
hostname(config-rtr)# router-id cluster-pool rpool
hostname(config-rtr)# interface gigabitEthernet0/0
hostname(config-rtr)# nameif inside
hostname(config-rtr)# security-level 0
hostname(config-rtr)# ip address 17.5.33.1 255.255.0.0 cluster-pool inside_pool
hostname(config-rtr)# ipv6 address 8888::1/64 cluster-pool p6
hostname(config-rtr)# ipv6 nd suppress-ra
hostname(config-rtr)# ipv6 ospf 2 area 0.0.0.0
```

Related Commands

Command	Description
ipv6 router ospf	Enters IPv6 router configuration mode.
router ospf	Enters router configuration mode.
show ipv6 ospf	Displays general information about the OSPFv3 routing processes.
show ospf	Displays general information about the OSPFv2 routing processes.

router eigrp

To start an EIGRP routing process and configure parameters for that process, use the **router eigrp** command in global configuration mode. To disable EIGRP routing, use the **no** form of this command.

router eigrp *as-number*

no router eigrp *as-number*

Syntax Description

as-number Autonomous system number that identifies the routes to the other EIGRP routers. It is also used to tag the routing information. Valid values are from 1 to 65535.

Defaults

EIGRP routing 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	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **router eigrp** command creates an EIGRP routing process or enters router configuration mode for an existing EIGRP routing process. You can only create a single EIGRP routing process on the ASA.

Use the following router configuration mode commands to configure the EIGRP routing processes:

- **auto-summary**—Enable/disable automatic route summarization.
- **default-information**—Enable/disable the reception and sending of default route information.
- **default-metric**—Define the default metrics for routes redistributed into the EIGRP routing process.
- **distance eigrp**—Configure the administrative distance for internal and external EIGRP routes.
- **distribute-list**—Filter the networks received and sent in routing updates.
- **eigrp log-neighbor-changes**—Enable/disable the logging of neighbor state changes.
- **eigrp log-neighbor-warnings**—Enable/disable the logging of neighbor warning messages.
- **eigrp router-id**—Creates a fixed router ID.
- **eigrp stub**—Configures the ASA for stub EIGRP routing.
- **neighbor**—Statically define an EIGRP neighbor.

- **network**—Configure the networks that participate in the EIGRP routing process.
- **passive-interface**—Configure an interface to act as a passive interface.
- **redistribute**—Redistribute routes from other routing processes into EIGRP.

Use the following interface configuration mode commands to configure interface-specific EIGRP parameters:

- **authentication key eigrp**—Define the authentication key used for EIGRP message authentication.
- **authentication mode eigrp**—Define the authentication algorithm used for EIGRP message authentication.
- **delay**—Configure the delay metric for an interface.
- **hello-interval eigrp**—Change the interval at which EIGRP hello packets are sent out of an interface.
- **hold-time eigrp**—Change the hold time advertised by the ASA.
- **split-horizon eigrp**—Enable/disable EIGRP split-horizon on an interface.
- **summary-address eigrp**—Manually define a summary address.

Examples

The following example shows how to enter the configuration mode for the EIGRP routing process with the autonomous system number 100:

```
hostname(config)# router eigrp 100  
hostname(config-rtr)#
```

Related Commands

Command	Description
clear configure eigrp	Clears the EIGRP router configuration mode commands from the running configuration.
show running-config router eigrp	Displays the EIGRP router configuration mode commands in the running configuration.

router ospf

To start an OSPF routing process and configure parameters for that process, use the **router ospf** command in global configuration mode. To disable OSPF routing, use the **no** form of this command.

```
router ospf pid
no router ospf pid
```

Syntax Description

<i>pid</i>	Internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535. The <i>pid</i> does not need to match the ID of OSPF processes on other routers.
------------	--

Defaults

OSPF routing 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	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

The **router ospf** command is the global configuration command for OSPF routing processes running on the ASA. Once you enter the **router ospf** command, the command prompt appears as (config-router)#, indicating that you are in router configuration mode.

When using the **no router ospf** command, you do not need to specify optional arguments unless they provide necessary information. The **no router ospf** command terminates the OSPF routing process specified by its *pid*. You assign the *pid* locally on the ASA. You must assign a unique value for each OSPF routing process.

The **router ospf** command is used with the following OSPF-specific commands to configure OSPF routing processes:

- **area**—Configures a regular OSPF area.
- **compatible rfc1583**—Restores the method used to calculate summary route costs per RFC 1583.
- **default-information originate**—Generates a default external route into an OSPF routing domain.
- **distance**—Defines the OSPF route administrative distances based on the route type.

- **ignore**—Suppresses the sending of syslog messages when the router receives a link-state advertisement (LSA) for type 6 Multicast OSPF (MOSPF) packets.
- **log-adj-changes**—Configures the router to send a syslog message when an OSPF neighbor goes up or down.
- **neighbor**—Specifies a neighbor router. Used to allow adjacency to be established over VPN tunnels.
- **network**—Defines the interfaces on which OSPF runs and the area ID for those interfaces.
- **redistribute**—Configures the redistribution of routes from one routing domain to another according to the parameters specified.
- **router-id**—Creates a fixed router ID.
- **summary-address**—Creates the aggregate addresses for OSPF.
- **timers lsa-group-pacing**—OSPF LSA group pacing timer (interval between group of LSA being refreshed or max-aged).
- **timers spf**—Delay between receiving a change to the SPF calculation.

Examples

The following example shows how to enter the configuration mode for the OSPF routing process numbered 5:

```
hostname(config)# router ospf 5
hostname(config-rtr)#
```

Related Commands

Command	Description
clear configure router	Clears the OSPF router commands from the running configuration.
show running-config router ospf	Displays the OSPF router commands in the running configuration.

router rip

To start a RIP routing process and configure parameters for that process, use the **router rip** command in global configuration mode. To disable the RIP routing process, use the **no** form of this command.

router rip

no router rip

Syntax Description

This command has no arguments or keywords.

Defaults

RIP routing 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	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **router rip** command is the global configuration command for configuring the RIP routing processes on the ASA. You can only configure one RIP process on the ASA. The **no router rip** command terminates the RIP routing process and removes all router configuration for that process.

When you enter the **router rip** command, the command prompt changes to hostname(config-router)#, indicating that you are in router configuration mode.

The **router rip** command is used with the following router configuration commands to configure RIP routing processes:

- **auto-summary**—Enable/disable automatic summarization of routes.
- **default-information originate**—Distribute a default route.
- **distribute-list in**—Filter networks in incoming routing updates.
- **distribute-list out**—Filter networks in outgoing routing updates.
- **network**—Add/remove interfaces from the routing process.
- **passive-interface**—Set specific interfaces to passive mode.
- **redistribute**—Redistribute routes from other routing processes into the RIP routing process.
- **version**—Set the RIP protocol version used by the ASA.

Additionally, you can use the following commands in interface configuration mode to configure RIP properties on a per-interface basis:

- **rip authentication key**—Set an authentication key.
- **rip authentication mode**—Set the type of authentication used by RIP Version 2.
- **rip send version**—Set the version of RIP used to send updates out of the interface. This overrides the version set in global router configuration mode, if any.
- **rip receive version**—Set the version of RIP accepted by the interface. This overrides the version set in global router configuration mode, if any.

RIP is not supported in transparent mode. By default, the ASA denies all RIP broadcast and multicast packets. To permit these RIP messages to pass through an ASA operating in transparent mode you must define access list entries to permit this traffic. For example, to permit RIP version 2 traffic through the ASA, create an access list entry such as the following:

```
hostname(config)# access-list myriplist extended permit ip any host 224.0.0.9
```

To permit RIP version 1 broadcasts, create an access list entry such as the following:

```
hostname(config)# access-list myriplist extended permit udp any any eq rip
```

Apply these access list entries to the appropriate interface using the **access-group** command.

You can enable both RIP and OSPF routing on the ASA at the same time.

Examples

The following example shows how to enter the configuration mode for the OSPF routing process numbered 5:

```
hostname(config)# router rip
hostname(config-rtr)# network 10.0.0.0
hostname(config-rtr)# version 2
```

Related Commands

Command	Description
clear configure router rip	Clears the RIP router commands from the running configuration.
show running-config router rip	Displays the RIP router commands in the running configuration.

rtp-conformance

To check RTP packets flowing on the pinholes for protocol conformance in H.323 and SIP, use the **rtp-conformance** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

rtp-conformance [enforce-payloadtype]

no rtp-conformance [enforce-payloadtype]

Syntax Description

enforce-payloadtype Enforces payload type to be audio/video based on the signaling exchange.

Defaults

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
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to check RTP packets flowing on the pinholes for protocol conformance on an H.323 call:

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# rtp-conformance
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
debug rtp	Displays debug information and error messages for RTP packets associated with H.323 and SIP inspection.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

rtp-min-port rtp-max-port

To configure the rtp-min-port and rtp-max-port limits for the phone proxy feature, use the **rtp-min-port** *port1* **rtp-max-port** *port2* command in phone-proxy configuration mode.

To remove the rtp-min-port and rtp-max-port limits from the phone proxy configuration, use the **no** form of this command.

rtp-min-port *port1* **rtp-maxport** *port2*

no rtp-min-port *port1* **rtp-maxport** *port2*

Syntax Description

<i>port1</i>	Specifies the minimum value for the RTP port range for the media termination point, where <i>port1</i> can be a value from 1024 to 16384.
<i>port2</i>	Specifies the maximum value for the RTP port range for the media termination point, where <i>port2</i> can be a value from 32767 to 65535.

Defaults

By default, the *port1* value for the **rtp-min-port** keyword is 16384 and the *port2* value for the **rtp-max-port** keyword is 32767.

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
Phone-proxy configuration	•	—	•	—	—

Command History

Release	Modification
8.2(1)	The command was introduced.

Usage Guidelines

Configure the RTP port range for the media termination point when you need to scale the number of calls that the Phone Proxy supports.

Examples

The following example shows the use of the **media-termination address** command to specify the IP address to use for media connections:

```
hostname(config-phone-proxy)# rtp-min-port 2001 rtp-maxport 32770
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

■ rtp-min-port rtp-max-port