



RADIUS Centralized Filter Management

First Published: November 25, 2005
Last Updated: February, 2006

The RADIUS Centralized Filter Management feature introduces a filter-server that acts as a centralized RADIUS repository for access control list (ACL) configuration. The filter-server works as a centralized administration point for ACL management.

History for the Radius Centralized Filter Management Feature

Release	Modification
12.2(13)T	This feature was introduced.
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Feature Overview, page 2](#)
- [Prerequisites, page 3](#)
- [Configuration Tasks, page 3](#)
- [Monitoring and Maintaining the Filter Cache, page 5](#)
- [Configuration Examples, page 5](#)
- [Additional References, page 8](#)
- [Command Reference, page 9](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2002–2003, 2005–2006 Cisco Systems, Inc. All rights reserved.

Feature Overview

Before the RADIUS Centralized Filter Management feature, wholesale providers (who provide premium charges for customer services such as access control lists [ACLs]) were unable to prevent customers from applying exhaustive ACLs, which could impact router performance and other customers. This feature introduces a centralized administration point—a filter server—for ACL management. The filter server acts as a centralized RADIUS repository for ACL configuration.

Whether or not the RADIUS server that is used as the filter server is the same server that is used for access authentication, the network access server (NAS) will initiate a second access request to the filter server. If configured, the NAS will use the filter-ID name as the authentication username and the filter server password for the second access request. The RADIUS server will attempt to authenticate the filter-ID name, returning any required filtering configuration in the access-accept response.

Because downloading ACLs is time consuming, a local cache is maintained on the NAS. If an ACL name exists on the local cache, that configuration will be used without consulting the filter server.

**Note**

An appropriately configured cache should minimize delays; however, the first dialin user to require a filter will always experience a longer delay because the ACL configuration is retrieved for the first time.

Cache Management

A global filter cache is maintained on the NAS of recently downloaded ACLs; thus, users no longer have to repeatedly request the same ACL configuration information from a potentially overloaded RADIUS server. Users are required to flush the cache when the following criteria have been met:

- After an entry becomes associated with a newly active call, the idle timer that is associated with that entry will be reset, if configured to do so.
- After the idle-time stamp of an entry expires, the entry will be removed.
- After the global cache of entries reaches a specified maximum number, the entry whose idle-timer is closest to the idle time limit will be removed.

A single timer is responsible for managing all cache entries. The timer is started after the first cache entry is created, and it runs periodically until reboot. The period of the timer will correspond to the minimum granularity offered when configuring cache idle timers, which is one expiration per minute. A single timer prevents users from having to manage individual timers per cache entry.

**Note**

The single timer introduces a lack of precision in timer expiration. There is an average error of approximately 50 percent of the timer granularity. Although decreasing the timer granularity will decrease the average error, the decreased timer granularity will negatively impact performance. Because precise timing is not required for cache management, the error delay should be acceptable.

New Vendor-Specific Attribute Support

This feature introduces support for three new vendor-specific attributes (VSAs), which can be divided into the following two categories:

- User profile extensions

- Filter-Required (50)—Specifies whether the call should be permitted if the specified filter is not found. If present, this attribute will be applied after any authentication, authorization, and accounting (AAA) filter method-list.
- Pseudo-user profile extensions
 - Cache-Refresh (56)—Specifies whether cache entries should be refreshed each time an entry is referenced by a new session. This attribute corresponds to the **cache refresh** command.
 - Cache-Time (57)—Specifies the idle time out, in minutes, for cache entries. This attribute corresponds to the **cache clear age** command.

**Note**

All RADIUS attributes will override any command-line interface (CLI) configurations.

Benefits

This feature allows users to centrally manage filters at a RADIUS server, thereby, offloading ACL configuration and management to a centralized repository.

Restrictions

Multiple method lists are not supported in this feature; only a single global filter method list can be configured.

Prerequisites

- You may need to add a dictionary file to your server if it does not support the new RADIUS VSAs. For a sample dictionary and vendors file, see the section “[RADIUS Dictionary and Vendors File Example](#)” later in this document.

If you need to add a dictionary file, ensure that your RADIUS server is nonstandard and that it can send the newly introduced VSAs.

- You want to set up RADIUS network authentication so a remote user can dial in and get IP connectivity.

Configuration Tasks

See the following sections for configuration tasks for the Centralized Filter Management feature. Each task in the list is identified as either required or optional.

- [Configuring the RADIUS ACL Filter Server](#) (required)
- [Configuring the Filter Cache](#) (required)
- [Verifying the Filter Cache](#) (optional)

Configuring the RADIUS ACL Filter Server

To enable the RADIUS ACL filter server, use the following command in global configuration mode:

Command	Purpose
<pre>Router(config)# aaa authorization cache filterserver default methodlist[methodlist2...]</pre>	<p>Enables AAA authorization caches and the downloading of an ACL configuration from a RADIUS filter server.</p> <ul style="list-style-type: none"> default—The default authorization list. methodlist [methodlist2...]—One of the keywords listed on the password command page.

Configuring the Filter Cache

To configure the filter cache, use the following commands beginning in global configuration:

	Command	Purpose
Step 1	<pre>Router(config)# aaa cache filter</pre>	Enables filter cache configuration and enters AAA filter configuration mode.
Step 2	<pre>Router(config-aaa-filter)# password {0 7} password</pre>	<p>(Optional) Specifies the optional password that is to be used for filter server authentication requests.</p> <p>0—Specifies that an unencrypted password will follow.</p> <p>7—Specifies that a hidden password will follow.</p> <p><i>password</i>—The unencrypted (clear text) password.</p> <p>Note If a password is not specified, the default password (“cisco”) is enabled.</p>
Step 3	<pre>Router(config-aaa-filter)# cache disable</pre>	(Optional) Disables the cache.
Step 4	<pre>Router(config-aaa-filter)# cache clear age minutes</pre>	<p>(Optional) Specifies, in minutes, when cache entries expire and the cache is cleared.</p> <p><i>minutes</i>—Any value between 0 to 4294967295.</p> <p>Note If a time is not specified, the default (1400 minutes [1 day]) is enabled.</p>
Step 5	<pre>Router(config-aaa-filter)# cache refresh</pre>	(Optional) Refreshes a cache entry when a new session begins. This command is enabled by default. To disable this functionality, use the no cache refresh command.
Step 6	<pre>Router(config-aaa-filter)# cache max number</pre>	<p>(Optional) Limits the absolute number of entries the cache can maintain for a particular server.</p> <p><i>number</i>—The maximum number of entries the cache can contain. Any value between 0 to 4294967295.</p> <p>Note If a number is not specified, the default (100 entries) is enabled.</p>

Verifying the Filter Cache

To display the cache status, use the **show aaa cache filterserver** EXEC command. The following is sample output for the **show aaa cache filterserver** command:

```
Router# show aaa cache filterserver
```

```
Filter      Server      Age Expires Refresh Access-Control-Lists
-----
aol         10.2.3.4    0    1440    100 ip in icmp drop
           ip out icmp drop
           ip out forward tcp dstip 1.2.3...
msn         10.3.3.4    N/A  Never    2 ip in tcp drop
msn2        10.4.3.4    N/A  Never    2 ip in tcp drop
vone        10.5.3.4    N/A  Never    0 ip in tcp drop
```



Note

The **show aaa cache filterserver** command shows how many times a particular filter has been referenced or refreshed. This function may be used in administration to determine which filters are actually being used.

Troubleshooting Tips

To help troubleshoot your filter cache configurations, use the privileged EXEC **debug aaa cache filterserver** command. To view sample output for the **debug aaa cache filterserver** command, refer to the section “[Debug Output Example](#)” later in this document.

Monitoring and Maintaining the Filter Cache

To monitor and maintain filter caches, use at least one of the following EXEC commands:

Command	Purpose
Router# clear aaa cache filterserver acl [<i>filter-name</i>]	Clears the cache status for a particular filter or all filters.
Router# show aaa cache filterserver	Displays the cache status.

Configuration Examples

This section provides the following configuration examples:

- [NAS Configuration Example, page 6](#)
- [RADIUS Server Configuration Example, page 6](#)
- [RADIUS Dictionary and Vendors File Example, page 6](#)
- [Debug Output Example, page 7](#)

NAS Configuration Example

The following example shows how to configure the NAS for cache filtering. In this example, the server group “mygroup” is contacted first. If there is no response, the default RADIUS server will then be contacted. If there still is no response, the local filters are contacted. Finally, the call is accepted if the filter cannot be resolved.

```
aaa authorization cache filterserver group mygroup group radius local none
!
aaa group server radius mygroup
  server 10.2.3.4
  server 10.2.3.5
!
radius-server host 10.1.3.4
!
aaa cache filter
  password mycisco
  no cache refresh
  cache max 100
!
```

RADIUS Server Configuration Example

The following example is a sample RADIUS configuration that is for a remote user “user1” dialing into the NAS:

```
myfilter Password = "cisco"
  Service-Type = Outbound,
  Ascend:Ascend-Call-Filter = "ip in drop srcip 10.0.0.1/32 dstip 10.0.0.10/32
  icmp",
  Ascend:Ascend-Call-Filter = "ip in drop srcip 10.0.0.1/32 dstip 10.0.0.10/32 tcp
  dstport = telnet",
  Ascend:Ascend-Cache-Refresh = Refresh-No,
  Ascend:Ascend-Cache-Time = 15

user1 Password = "cisco"
  Service-Type = Framed,
  Filter-Id = "myfilter",
  Ascend:Ascend-Filter-Required = Filter-Required-Yes,
```

RADIUS Dictionary and Vendors File Example

The following example is a sample RADIUS dictionary file for the new VSAs. In this example, the dictionary file is for a Merit server.

```
dictionary file:
Ascend.attr Ascend-Filter-Required 50 integer (*, 0, NOENCAPS)
Ascend.attr Ascend-Cache-Refresh 56 integer (*, 0, NOENCAPS)
Ascend.attr Ascend-Cache-Time 57 integer (*, 0, NOENCAPS)

Ascend.value Ascend-Cache-Refresh Refresh-No 0
Ascend.value Ascend-Cache-Refresh Refresh-Yes 1

Ascend.value Ascend-Filter-Required Filter-Required-No 0
Ascend.value Ascend-Filter-Required Filter-Required-Yes 1

vendors file:
```

```
50      50
56      56
57      57
```

Debug Output Example

The following is sample output from the **debug aaa cache filterserver** command:

```
Router# debug aaa cache filterserver

AAA/FLTSV: need "myfilter" (fetch), call 0x612DAC64
AAA/FLTSV: send req, call 0x612DAC50
AAA/FLTSV: method SERVER_GROUP myradius
AAA/FLTSV: recv reply, call 0x612DAC50 (PASS)
AAA/FLTSV: create cache
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: skip attr "filter-cache-refresh"
AAA/FLTSV: skip attr "filter-cache-time"
AAA/CACHE: set "AAA filtserv cache" entry "myfilter" refresh? no
AAA/CACHE: set "AAA filtserv cache" entry "myfilter" cachetime 15
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: PASS call 0x612DAC64
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (1 entry)
AAA/CACHE: destroy "AAA filtserv cache" entry "myfilter"
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)
```

Additional References

The following sections provide references related to RADIUS Centralized Filter Management.

Related Documents

Related Topic	Document Title
Configuring Authorization	“Configuring Authorization” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Configuring RADIUS	“Configuring RADIUS” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Authorization Commands	“Authorization Commands” section in the <i>Cisco IOS Security Command Reference</i> , Release 12.4

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents modified commands only.

- [aaa authorization cache filterserver](#)
- [aaa cache filter](#)
- [cache clear age](#)
- [cache disable](#)
- [cache refresh](#)
- [clear aaa cache filterserver acl](#)
- [debug aaa cache filterserver](#)
- [password](#)
- [show aaa cache filterserver](#)

aaa authorization cache filterserver

To enable authentication, authorization, and accounting (AAA) authorization caches and the downloading of access control list (ACL) configurations from a RADIUS filter server, use the **aaa authorization cache filterserver** command in global configuration mode. To disable AAA authorization caches, use the **no** form of this command.

aaa authorization cache filterserver default *methodlist* [*methodlist2...*]

no aaa authorization cache filterserver default

Syntax Description

default	Default authorization list.
<i>methodlist</i> [<i>methodlist2...</i>]	One of the keywords listed in Table 1 .

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use the **aaa authorization cache filterserver** command to enable the RADIUS ACL filter server. Method keywords are described in [Table 1](#).

Table 1 *aaa authorization cache filterserver Methods*

Keyword	Description
group <i>group-name</i>	Uses a subset of RADIUS servers for authentication as defined by the aaa group server radius command.
local	Uses the local database for authorization caches and ACL configuration downloading.
none	No authorization is performed.

This command functions similarly to the **aaa authorization** command with the following exceptions:

- Named method-lists cannot be configured.
- Only one instance of this command can be configured.
- TACACS+ groups cannot be configured.

Examples

The following example shows how to configure the default RADIUS server group as the desired filter. If the request is rejected or a reply is not returned, local configuration will be consulted. If the local filter does not respond, the call will be accepted but filtering will not occur.

```
aaa authorization cache filterserver group radius local none
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.

aaa cache filter

To enable filter cache configuration, use the **aaa cache filter** command in global configuration mode. To disable this functionality, use the **no** form of this command.

aaa cache filter

no aaa cache filter

Syntax Description

This command has no arguments or keywords.

Defaults

Filter cache configuration is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use the **aaa cache filter** command to begin filter cache configuration and enter AAA filter configuration mode (config-aaa-filter).

After enabling this command, you can specify filter cache parameters with the following commands:

- **cache clear age**—Specifies, in minutes, when cache entries expire and the cache is cleared.
- **cache disable**—Disables the cache.
- **cache max**—Refreshes a cache entry when a new sessions begins.
- **cache refresh**—Limits the absolute number of entries the cache can maintain for a particular server.
- **password**—Specifies the optional password that is to be used for filter server authentication requests.



Note

Each of these commands is optional; thus, the default value will be enabled for any command that is not specified.

Examples

The following example shows how to enable filter cache configuration and specify cache parameters.

```
aaa cache filter
password mycisco
no cache refresh
cache max 100
```

Related Commands

Command	Description
aaa authorization cache filterserver	Enables AAA authorization caches and the downloading of ACL configurations from a RADIUS filter server.
cache clear age	Specifies when, in minutes, cache entries expire and the cache is cleared.
cache disable	Disables the cache.
cache max	Refreshes a cache entry when a new sessions begins.
cache refresh	Limits the absolute number of entries the cache can maintain for a particular server.
password	Specifies the optional password that is to be used for filter server authentication requests.

cache clear age

To specify when, in minutes, cache entries expire and the cache is cleared, use the **cache clear age** command in AAA filter configuration mode. To return to the default value, use the **no** form of this command.

cache clear age *minutes*

no cache clear age

Syntax Description	<i>minutes</i>	Any value from 0 to 4294967295; the default value is 1440 minutes.
---------------------------	----------------	--

Defaults	1440 minutes (1 day)
-----------------	----------------------

Command Modes	AAA filter configuration
----------------------	--------------------------

Command History	Release	Modification
	12.2(13)T	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines	After enabling the aaa cache filter command, which allows you to configure cache filter parameters, you can use the cache clear age command to specify when cache entries should expire. If this command is not specified, the default value (1440 minutes) will be enabled.
-------------------------	--

Examples	The following example shows how to configure the cache entries to expire every 60 minutes:
-----------------	--

```
aaa cache filter
cache clear age 60
```

Related Commands	Command	Description
	aaa cache filter	Enables filter cache configuration.

cache disable

To disable the cache, use the **cache disable** command in AAA filter configuration mode. To return to the default, use the **no** form of this command.

cache disable

no cache disable

Syntax Description This command has no arguments or keywords.

Defaults Caching is enabled.

Command Modes AAA filter configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines After enabling the **aaa cache filter** command, which allows you to configure cache filter parameters, you can use the **cache disable** command to disable filter caching. This command can be used to verify that the access control lists (ACLs) are being downloaded.

Examples The following example shows how to disable filter caching:

```
aaa cache filter
cache disable
```

Related Commands	Command	Description
	aaa cache filter	Enables filter cache configuration.

cache refresh

To refresh a cache entry after a new session begins, use the **cache refresh** command in AAA filter configuration mode. To disable this functionality, use the **no** form of this command.

cache refresh

no cache refresh

Syntax Description This command has no arguments or keywords.

Defaults This command is enabled by default.

Command Modes AAA filter configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **cache refresh** command is used in an attempt to keep cache entries from the filter server, that are being referred to by new sessions, within the cache. This command resets the idle timer for these entries when they are referenced by new calls.

Examples

The following example shows how to disable the **cache refresh** command:

```
aaa cache filter
 password mycisco
 no cache refresh
 cache max 100
```

Related Commands

Command	Description
aaa cache filter	Enables filter cache configuration.

clear aaa cache filterserver acl

To clear the cache status for a particular filter or all filters, use the **clear aaa cache filterserver acl** command in EXEC mode.

```
clear aaa cache filterserver acl [filter-name]
```

Syntax Description	<i>filter-name</i> (Optional) Cache status of a specified filter is cleared.
---------------------------	--

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.	

Usage Guidelines	After you clear the cache status for a particular filter or all filters, it is recommended that you enable the show aaa cache filterserver command to verify that the cache status.
-------------------------	--

Examples	The following example shows how to clear the cache for all filters:
-----------------	---

```
clear aaa cache filterserver acl
```

Related Commands	Command	Description
	show aaa cache filterserver	Displays the cache status.

debug aaa cache filterserver

To help troubleshoot your filter cache configurations, use the **debug aaa cache filterserver** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug aaa cache filterserver

no debug aaa cache filterserver

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(13)T	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB

Examples The following is sample output from the **debug aaa cache filterserver** command:

```
Router# debug aaa cache filterserver

AAA/FLTSV: need "myfilter" (fetch), call 0x612DAC64
AAA/FLTSV: send req, call 0x612DAC50
AAA/FLTSV: method SERVER_GROUP myradius
AAA/FLTSV: rcv reply, call 0x612DAC50 (PASS)
AAA/FLTSV: create cache
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: skip attr "filter-cache-refresh"
AAA/FLTSV: skip attr "filter-cache-time"
AAA/CACHE: set "AAA filtserv cache" entry "myfilter" refresh? no
AAA/CACHE: set "AAA filtserv cache" entry "myfilter" cachetime 15
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: PASS call 0x612DAC64
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (1 entry)
AAA/CACHE: destroy "AAA filtserv cache" entry "myfilter"
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)
```

Related Commands	Command	Description
	aaa authorization cache filterserver	Enables AAA authorization caches and the downloading of ACL configurations from a RADIUS filter server.

password

To configure the password used by a provider edge (PE) router for Challenge Handshake Authentication Protocol (CHAP) style Layer 2 Tunnel Protocol Version 3 (L2TPv3) authentication, use the **password** command in L2TP class configuration mode. To disable a configured password, use the **no** form of this command.

```
password [0 | 7] password
```

```
no password
```

Syntax Description	[0 7]	(Optional) Specifies the input format of the shared secret.
		<ul style="list-style-type: none"> 0—Specifies that a plain-text secret will be entered. 7—Specifies that an encrypted secret will be entered.
		The default value is 0 .
	<i>password</i>	The password used for L2TPv3 authentication.

Defaults If a password is not configured for the L2TP class with the **password** command, the password configured with the **username password** command in global configuration mode is used. The default input format of the shared secret is **0**.

Command Modes L2TP class configuration

Command History	Release	Modification
	12.0(23)S	This command was introduced.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines The password hierarchy sequence used for a local and remote peer PE for L2TPv3 authentication is as follows:

- The L2TPv3 password (configured with the **password** command) is used first.
- If no L2TPv3 password exists, the globally configured password (configured with the **username password** command) for the router is used.

Examples The following example sets the password named tunnel2 to be used to authenticate an L2TPv3 session between the local and remote peers in L2TPv3 pseudowires configured with the L2TP class configuration named l2tp class1:

```
Router(config)# l2tp-class l2tp-class1
Router(config-l2tp-class)# authentication
Router(config-l2tp-class)# password tunnel2
```

password

Related Commands

Command	Description
authentication	Enables L2TPv3 CHAP-style authentication.
l2tp-class	Creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes and enters L2TP class configuration mode.

show aaa cache filterserver

To display the cache status, use the **show aaa cache filterserver** command in EXEC mode.

show aaa cache filterserver

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	12.2(13)T	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines The **show aaa cache filterserver** command shows how many times a particular filter has been referenced or refreshed. This function may be used in administration to determine which filters are actually being used.

Examples The following is sample output for the **show aaa cache filterserver** command:

```
Router# show aaa cache filterserver

Filter      Server      Age Expires Refresh Access-Control-Lists
-----
aol         10.2.3.4    0    1440    100 ip in icmp drop
           ip out icmp drop
           ip out forward tcp dstip 1.2.3...
msn         10.2.3.4    N/A  Never    2 ip in tcp drop
msn2        10.2.3.4    N/A  Never    2 ip in tcp drop
vone        10.2.3.4    N/A  Never    0 ip in tcp drop
```

[Table 2](#) describes the significant fields shown in the display.

Table 2 *show aaa cache filterserver Field Descriptions*

Field	Description
Filter	Filter name.
Server	RADIUS server IP address.
Age	When to expire a cache entry.
Expires	Number of minutes in which a cache entry will expire.
Refresh	Number of times a cache has been refreshed.
Access-Control-Lists	Access control list (ACL) of the server.

```
show aaa cache filterserver
```

Related Commands

Command	Description
aaa authorization cache filterserver	Enables AAA authorization caches and the downloading of ACL configurations from a RADIUS filter server.

CCVP, the Cisco logo, and welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the way we work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2002–2003, 2005–2006 Cisco Systems, Inc. All rights reserved.