AAA Authorization and Authentication Cache

First Published: March 16, 2006
Last Updated: March 1, 2006

The AAA Authorization and Authentication Cache feature allows you to cache authorization and authentication responses for a configured set of users or service profiles, providing performance improvements and an additional level of network reliability because user and service profiles that are returned from authorization and authentication responses can be queried from multiple sources and need not depend solely on an offload server. This feature also provides a failover mechanism so that if a network RADIUS or TACACS+ server is unable to provide authorization and authentication responses network users and administrators can still access the network.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Implementing Authorization and Authentication Profile Caching" section on page 33".

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

CISCO SYSTEMS

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

Prerequisites for Implementing Authorization and Authentication Profile Caching

The following prerequisites apply to implementing authorization and authentication profile caching:

- Understand how you would want to implement profile caching, that is, are profiles being cached to improve network performance or as a failover mechanism if your network authentication and authorization (RADIUS and TACACS+) servers become unavailable.
- RADIUS and TACACS+ server groups must already be configured.

Information About Implementing Authorization and Authentication Profile Caching

To implement authorization and authentication profile caching, you should understand the following concepts:

Network Performance Optimization Using Authorization and Authentication Profile Caching

RADIUS and TACACS+ clients run on Cisco routers and send authentication requests to a central RADIUS or TACACS+ server that contains all user authentication and network service access information. The router is required to communicate with an offload RADIUS or TACACS+ server to authenticate a given call and then apply a policy or service to that call. Unlike authentication, authorization, and accounting (AAA) accounting, AAA authentication and authorization is a blocking procedure, which means the call setup may not proceed while the call is being authenticated and authorized. Thus, the time required to process the call setup is directly impacted by the time required to process such an authentication or authorization request from the router to the offload RADIUS or TACACS+ server, and back again. Any communication problems in the transmission, offload server utilization, and numerous other factors cause significant degradation in a router's call setup performance due simply to the AAA authentication and authorization step. The problem is further highlighted when multiple AAA authentications and authorizations are needed for a single call or session.

A solution to this problem is to minimize the impact of such authentication requests by caching the authentication and authorization responses for given users on the router, thereby removing the need to send the requests to an offload server again and again. This profile caching adds significant performance improvements to call setup times. Profile caching also provides an additional level of network reliability because user and service profiles that are returned from authentication and authorization responses can be queried from multiple sources and need not depend solely on an offload server.

To take advantage of this performance optimization, you need to configure the authentication method list so that the AAA cache profile is queried first when a user attempts to authenticate to the router. See the "Method Lists in Authorization and Authentication Profile Caching" section for more information.

Authorization and Authentication Profile Caching as a Failover Mechanism

If, for whatever reason, RADIUS or TACACS+ servers are unable to provide authentication and authorization responses, network users and administrators can be locked out of the network. The profile caching feature allows usernames to be authorized without having to complete the authentication phase. For example, a user by the name of user100@abc.com with a password secretpassword1 could be stored in a profile cache using the regular expression ".*@abc.com". Another user by the name of user101@abc.com with a password of secretpassword2 could also be stored using the same regular expression, and so on. Because the number of users in the ".*@abc.com" profile could number in the thousands, it is not feasible to authenticate each user with their personal password. Therefore authentication is disabled and each user simply accesses authorization profiles from a common Access Response stored in cache.

The same reasoning applies in cases where higher end security mechanisms such as Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), or Extensible Authentication Protocol (EAP), which all use an encrypted password between the client and AAA offload server, are used. To allow these unique, secure username and password profiles to retrieve their authorization profiles, authentication is bypassed.

To take advantage of this failover capability, you need to configure the authentication and authorization method list so that the cache server group is queried last when a user attempts to authenticate to the router. See the "Method Lists in Authorization and Authentication Profile Caching" section for more information.

Method Lists in Authorization and Authentication Profile Caching

A method list is a sequential list describing the authentication methods to be queried in order to authenticate a user. We support methods such as local (use the local Cisco IOS database), none (do nothing), RADIUS server group, or TACACS+ server group. Typically, more than one method can be configured into a method list. Cisco IOS software uses the first listed method to authenticate users. If that method fails to respond, the Cisco IOS software selects the next authentication method listed in the method list. This process continues until there is successful communication with a listed authentication method, or until all methods defined in the method list are exhausted.

To optimize network performance or provide failover capability using the profile caching feature you simply change the order of the authentication and authorization methods in the method list. To optimize network performance, make sure the cache server group appears first in the method list. For failover capability, the cache server group should appear last in the method list.

Authorization and Authentication Profile Caching Guidelines

Because the number of usernames and profiles that can request to be authenticated or authorized at a given router on a given point of presence (POP) can be quite extensive, it would not be feasible to cache all of them. Therefore, only usernames and profiles that are commonly used or that share a common authentication and authorization response should be configured to use caching. Commonly used usernames such as aolip and aolnet, which are used for America Online (AOL) calls, or preauthentication dialed number identification service (DNIS) numbers used to connect Public Switched Telephone

Network (PSTN) calls to a network attached storage device, along with domain-based service profiles, are all examples of usernames and profiles that can benefit from authentication and authorization caching.

General Configuration Procedure for Implementing Authorization and Authentication Profile Caching

To implement authorization and authentication profile caching, you would complete the following procedure:

1. Create cache profile groups and define the rules for what information is cached in each group.

   Entries that match based on exact username, regular expressions, or specify that all authentication and authorization requests can be cached.
2. Update existing server groups to reference newly defined cache groups.
3. Update authentication or authorization method lists to use the cached information to optimize network performance or provide a failover mechanism.

How to Implement Authorization and Authentication Profile Caching

This section contains the following tasks:

- Creating Cache Profile Groups and Defining Caching Rules, page 4 (required)
- Defining RADIUS and TACACS+ Server Groups That Use Cache Profile Group Information, page 7 (required)
- Updating Authorization and Authentication Method Lists to Specify How Cache Information is Used, page 8 (required)

Creating Cache Profile Groups and Defining Caching Rules

Perform this task to create a cache profile group, define the rules for what information is cached in that group, and verify and manage cache profile entries.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa cache profile** *group-name*
5. **profile** *name* [**no-auth**]
6. Repeat Step 5 for each username you want to add to the profile group in Step 4.
7. **regexp** *matchexpression* {**any** | **only**} [**no-auth**]

8. Repeat Step 7 for each regular expression you want to add to the cache profile group defined in Step 4.
9. **all** [**no-auth**]
10. **end**
11. **show aaa cache group** *name*
12. **clear aaa cache group** *name* {**profile** *name* | **all**}
13. **debug aaa cache group**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA access control model.
Step 4	**aaa cache profile** *group-name* **Example:** `Router(config)# aaa cache profile networkusers@companyname`	Defines an authentication and authorization cache profile server group and enters profile map configuration mode.
Step 5	**profile** *name* [**no-auth**] **Example:** `Router(config-profile-map# profile networkuser1 no-auth`	Creates an individual authentication and authorization cache profile based on a username match. • The *name* argument must be an exact match to a username being queried by an authentication or authorization service request. • Use the **no-auth** keyword to bypass authentication for this user.
Step 6	Repeat Step 5 for each username you want to add to the profile group in Step 4.	—

	Command or Action	Purpose
Step 7	**regexp** *matchexpression* {**any** | **only**} [**no-auth**] **Example:** `Router(config-profile-map)# regexp .*@abc.com any no-auth`	(Optional) Creates an entry in a cache profile group that matches based on a regular expression. • If you use the **any** keyword, all unique usernames matching the regular expression are saved. • If you use the **only** keyword, only one profile entry is cached for all usernames matching the regular expression. • Use the **no-auth** keyword to bypass authentication for this user or set of users. • Because the number of entries in a regular expression cache profile group could be in the thousands, and validating each request against a regular expression can be time consuming, we do not recommend using regular expression entries in cache profile groups.
Step 8	Repeat Step 7 for each regular expression you want to add to the cache profile group defined in Step 4.	—
Step 9	**all** [**no-auth**] **Example:** `Router(config-profile-map)# all no-auth`	(Optional) Specifies that all authentication and authorization requests are cached. • Use the **all** command for specific service authorization requests, but it should be avoided when dealing with authentication requests.
Step 10	**end** **Example:** `Router(config-profile-map)# end`	Returns to privileged EXEC mode.
Step 11	**show aaa cache group** *name* **Example:** `Router# show aaa cache group networkusers@companyname`	(Optional) Displays all cache entries for a specified group.
Step 12	**clear aaa cache group** *name* {**profile** *name* | **all**} **Example:** `Router# clear aaa cache group networkusers@companyname profile networkuser1`	(Optional) Clears an individual entry or all entries in the cache.
Step 13	**debug aaa cache group** **Example:** `Router# debug aaa cache group`	(Optional) Displays debug information about cached entries.

Defining RADIUS and TACACS+ Server Groups That Use Cache Profile Group Information

Perform this task to define how RADIUS and TACACS+ server groups use the information stored in each cache profile group.

Prerequisites

RADIUS and TACACS+ server groups must be created.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *group-name*
   or
   aaa group server tacacs+ *group-name*
5. **cache authorization profile** *name*
6. **cache authentication profile** *name*
7. **cache expiry** *hours* [**enforce** | **failover**]
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA access control model.
Step 4	**aaa group server radius** *group-name* or **aaa group server tacacs+** *group-name* **Example:** `Router(config)# aaa group server radius networkusers@companyname`	Enters RADIUS server group configuration mode. • To enter TACACS+ server group configuration mode, use the **aaa group server tacacs+** *group-name* command.

	Command or Action	Purpose
Step 5	**cache authorization profile** *name* **Example:** `Router(config-sg-radius)# cache authorization profile networkusers@companyname`	Activates the authorization caching rules in the profile networkusers for this RADIUS or TACACS+ server group. • The *name* argument in this command is a AAA cache profile group name.
Step 6	**cache authentication profile** *name* **Example:** `Router(config-sg-radius)# cache authentication profile networkusers@companyname`	Activates the authentication caching rules in the profile networkusers for this RADIUS or TACACS+ server group.
Step 7	**cache expiry** *hours* {**enforce** | **failover**} **Example:** `Router(config-sg-radius)# cache expiry 240 failover`	(Optional) Sets the amount of time before a cache profile entry expires (becomes stale). • Use the **enforce** keyword to specify that once a cache profile entry expires it is not used again. • Use the **failover** keyword to specify that an expired cache profile entry can be used if all other methods to authenticate and authorize the user fail.
Step 8	**end** **Example:** `Router(config-sg-radius)# end`	Returns to privileged EXEC mode.

Updating Authorization and Authentication Method Lists to Specify How Cache Information is Used

Perform this task to update authorization and authentication method lists to use the authorization and authentication cache information.

Prerequisites

Method lists must already be defined.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2*...]]
5. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2*...]
6. **aaa authentication login** {**default** | *list-name*} *method1* [*method2*...]
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA access control model.
Step 4	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2*...]] **Example:** `Router(config)# aaa authorization network default cache networkusers@companyname group networkusers@companyname`	Enables AAA authorization and creates method lists, which define the authorization methods used when a user accesses a specified function.
Step 5	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2*...] **Example:** `Router(config)# aaa authentication ppp default cache networkusers@companyname group networkusers@companyname`	Specifies one or more authentication methods for use on serial interfaces that are running PPP.
Step 6	**aaa authentication login** {**default** | *list-name*} *method1* [*method2*...] **Example:** `Router(config)# aaa authentication login default cache adminusers group adminusers`	Sets the authentication at login.
Step 7	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Configuration Examples for Implementing Authorization and Authentication Profile Caching

This section contains the following examples:

- Implementing Authorization and Authentication Profile Caching for Network Optimization: Example, page 10

- Implementing Authorization and Authentication Profile Caching as a Failover Mechanism: Example, page 10

Implementing Authorization and Authentication Profile Caching for Network Optimization: Example

The following configuration example shows how to:

- Define a cache profile group adminusers that contains all administrator names on the network and sets it as the default list that is used for all login and exec sessions.
- Activate the new caching rules for a RADIUS server group.
- Add the new cache profile group in the authentication and authorization method list and change the method order so that the cache profile group is queried first.

```
configure terminal
 aaa new-model
 ! Define aaa cache profile groups and the rules for what information is saved to cache.
 aaa cache profile admin_users
 profile adminuser1
 profile adminuser2
 profile adminuser3
 profile adminuser4
 profile adminuser5
 exit
 ! Define server groups that use the cache information in each profile group.
 aaa group server radius admins@companyname.com
 cache authorization profile admin_users
 cache authentication profile admin_users
 ! Update authentication and authorization method lists to specify how profile groups and
server groups are used.
 aaa authentication login default cache admins@companyname.com group
admins@companyname.com
 aaa authorization exec default cache admins@companyname.com group admins@companyname.com
 end
```

Implementing Authorization and Authentication Profile Caching as a Failover Mechanism: Example

The following configuration example shows how to:

- Create a cache profile group admin_users that contains all of the administrators on the network so that if the RADIUS or TACACS+ server should become unavailable the administrators can still access the network.
- Create a cache profile group abc_users that contains all of the ABC company users on the network so that if the RADIUS or TACACS+ server should become unavailable these users will be authorized to use the network.
- Activate the new caching rules for each profile group on a RADIUS server.

- Add the new cache profile group in the authentication and authorization method list and change the method order so that the cache profile group is queried last.

```
configure terminal
 aaa new-model
 ! Define aaa cache profile groups and the rules for what information is saved to cache.
 aaa cache profile admin_users
 profile admin1
 profile admin2
 profile admin3
 exit
 aaa cache profile abcusers
 profile .*@abc.com only no-auth
 exit
 ! Define server groups that use the cache information in each cache profile group.
 aaa group server tacacs+ admins@companyname.com
 server 10.1.1.1
 server 10.20.1.1
 cache authentication profile admin_users
 cache authorization profile admin_users
 exit
 aaa group server radius abcusers@abc.com
 server 172.16.1.1
 server 172.20.1.1
 cache authentication profile abcusers
 cache authorization profile abcusers
 exit
 ! Update authentication and authorization method lists to specify how cache is used.
 aaa authentication login default cache admins@companyname.com group
admins@companyname.com
 aaa authorization exec default cache admins@companyname.com group admins@companyname.com
 aaa authentication ppp default group abcusers@abc.com cache abcusers@abc.com
 aaa authorization network default group abcusers@abc.com cache abcusers@abc.com
 end
```

Additional References

The following sections provide references related to implementing authentication and authorization profile caching.

Related Documents

Related Topic	Document Title
Authentication configuring tasks	"Configuring Authentication" chapter in the *Cisco IOS Security Configuration Guide*, Release 12.2
Authorization configuration tasks	"Configuring Authorization" chapter in the *Cisco IOS Security Configuration Guide*, Release 12.2
RADIUS configuration tasks	"Configuring RADIUS" chapter in the *Cisco IOS Security Configuration Guide*, Release 12.2

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support 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 new and modified commands only.

New Commands

- **aaa cache profile**
- **all (profile map configuration)**
- **cache authentication profile (server group configuration)**
- **cache authorization profile (server group configuration)**
- **cache expiry (server group configuration)**

- clear aaa cache group
- debug aaa cache group
- profile (profile map configuration)
- regexp (profile map configuration)
- show aaa cache group

Modified Commands

- aaa authentication login
- aaa authentication ppp
- aaa authorization

aaa authentication login

To set authentication, authorization, and accounting (AAA) authentication at login, use the **aaa authentication login** command in global configuration mode. To disable AAA authentication, use the **no** form of this command.

aaa authentication login {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication login {**default** | *list-name*} *method1* [*method2*...]

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods activated when a user logs in.
method1 [*method2*...]	Identifies the list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. Method keywords described in Table 1.

Defaults

If the **default** list is not set, only the local user database is checked. This has the same effect as the following command:

```
aaa authentication login default local
```

Note On the console, login will succeed without any authentication checks if **default** is not set.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	The **group radius**, **group tacacs+**, and **local-case** keywords were added as methods for authentication.
12.2(28)SB	The **cache** *group-name* keyword and argument were added as a method for authentication.

Usage Guidelines

The default and optional list names that you create with the **aaa authentication login** command are used with the **login authentication** command.

Create a list by entering the **aaa authentication login** *list-name method* command for a particular protocol, where *list-name* is any character string used to name this list (such as MIS-access). The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence. Method keywords are described in Table 1.

To create a default list that is used if no list is assigned to a line, use the **login authentication** command with the default argument followed by the methods you want to use in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

If authentication is not specifically set for a line, the default is to deny access and no authentication is performed. Use the **more system:running-config** command to display currently configured lists of authentication methods.

Note In Table 1, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Table 1 aaa authentication login Methods

Keyword	Description
enable	Uses the enable password for authentication.
krb5	Uses Kerberos 5 for authentication.
krb5-telnet	Uses Kerberos 5 telnet authentication protocol when using Telnet to connect to the router.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
cache *group-name*	Uses a cache server group for authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

Examples

The following example creates an AAA authentication list called *MIS-access*. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication login MIS-access group tacacs+ enable none
```

The following example creates the same list, but it sets it as the default list that is used for all login authentications if no other list is specified:

```
aaa authentication login default group tacacs+ enable none
```

The following example sets authentication at login to use the Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router:

```
aaa authentication login default krb5
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
login authentication	Enables AAA authentication for logins.

aaa authentication ppp

To specify one or more authentication, authorization, and accounting (AAA) authentication methods for use on serial interfaces that are running PPP, use the **aaa authentication ppp** command in global configuration mode. To disable authentication, use the **no** form of this command.

aaa authentication ppp {**default** | *list-name*} *method1* [*method2*...]

no aaa authentication ppp {**default** | *list-name*} *method1* [*method2*...]

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods tried when a user logs in.
method1 [*method2*...]	Identifies the list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. Method keywords are described in Table 2.

Defaults

If the **default** list is not set, only the local user database is checked. This has the same effect as that created by the following command:

```
aaa authentication ppp default local
```

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server support and **local-case** were added as method keywords.

Usage Guidelines

The lists that you create with the **aaa authentication ppp** command are used with the **ppp authentication** command. These lists contain up to four authentication methods that are used when a user tries to log in to the serial interface.

Create a list by entering the **aaa authentication ppp** *list-name method* command, where *list-name* is any character string used to name this list (such as *MIS-access*). The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence. You can enter up to four methods. Method keywords are described in Table 2.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to have authentication succeed even if all methods return an error.

If authentication is not specifically set for a function, the default is **none** and no authentication is performed. Use the **more system:running-config** command to display currently configured lists of authentication methods.

Note In Table 2, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Table 2 aaa authentication ppp Methods

Keyword	Description
if-needed	Does not authenticate if the user has already been authenticated on a tty line.
krb5	Uses Kerberos 5 for authentication (can be used only for Password Authentication Protocol [PAP] authentication).
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
cache *group-name*	Uses a cache server group for authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

Examples

The following example creates a AAA authentication list called *MIS-access* for serial lines that use PPP. This authentication first tries to contact a TACACS+ server. If this action returns an error, the user is allowed access with no authentication.

```
aaa authentication ppp MIS-access group tacacs+ none
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa group server tacacs+	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
more system:running-config	Displays the contents of the currently running configuration file, the configuration for a specific interface, or map class information.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server host	Specifies a RADIUS server host.
tacacs+-server host	Specifies a TACACS host.

aaa authorization

To set parameters that restrict user access to a network, use the **aaa authorization** command in global configuration mode. To disable authorization for a function, use the **no** form of this command.

aaa authorization {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]

no aaa authorization {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration** | **default** | *list-name*}

Syntax Description

network	Runs authorization for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Programs (NCPs), and AppleTalk Remote Access (ARA).
exec	Runs authorization to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as autocommand information.
commands	Runs authorization for all commands at the specified privilege level.
level	Specific command level that should be authorized. Valid entries are 0 through 15.
reverse-access	Runs authorization for reverse access connections, such as reverse Telnet.
configuration	Downloads the configuration from the authentication, authorization, and accounting (AAA) server.
default	Uses the listed authorization methods that follow this keyword as the default list of methods for authorization.
list-name	Character string used to name the list of authorization methods.
method1 [*method2...*]	Identifies an authorization method or multiple authorization methods to be used for authorization. A method may be any one of the keywords listed in Table 3.

Defaults

Authorization is disabled for all actions (equivalent to the method keyword **none**).

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	The **group radius** and **group tacacs+** keywords were added as methods for authorization.
12.2(28)SB	The **cache** *group-name* keyword and argument were added as a method for authorization.

Usage Guidelines

Use the **aaa authorization** command to enable authorization and to create named methods lists, defining authorization methods that can be used when a user accesses the specified function. Method lists for authorization define the ways authorization will be performed and the sequence in which these methods

will be performed. A method list is a named list describing the authorization methods to be used (such as RADIUS or TACACS+), in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted.

Note The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle—meaning that the security server or local username database responds by denying the user services—the authorization process stops and no other authorization methods are attempted.

If the **aaa authorization** command for a particular authorization type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this authorization type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no authorization takes place.

Use the **aaa authorization** command to create a list by entering values for the *list-name* and the *method* arguments, where *list-name* is any character string used to name this list (excluding all method names) and *method* identifies the list of authorization methods tried in the given sequence.

Note In Table 3, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Method keywords are described in Table 3.

Table 3 aaa authorization Methods

Keyword	Description
cache *group-name*	Uses a cache server group for authorization.
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the **server group** *group-name* command.
if-authenticated	Allows the user to access the requested function if the user is authenticated.
krb5-instance	Uses the instance defined by the **kerberos instance map** command.
local	Uses the local database for authorization.
none	No authorization is performed.

Cisco IOS software supports the following methods for authorization:

- Cache Sever Groups—The router consults its cache server groups to authorize specific rights for users.
- RADIUS—The network access server requests authorization information from the RADIUS security server group. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.
- TACACS+—The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value (AV) pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.
- If-Authenticated—The user is allowed to access the requested function provided the user has been authenticated successfully.
- None—The network access server does not request authorization information; authorization is not performed over this line or interface.
- Local—The router or access server consults its local database, as defined by the **username** command, to authorize specific rights for users. Only a limited set of functions can be controlled via the local database.
- Kerberos Instance Map—The network access server uses the instance defined by the **kerberos instance map** command for authorization.

Method lists are specific to the type of authorization being requested. AAA supports five different types of authorization:

- Network—Applies to network connections. This can include a PPP, SLIP, or ARA connection.
- EXEC—Applies to the attributes associated with a user EXEC terminal session.
- Commands—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- Reverse Access—Applies to reverse Telnet sessions.
- Configuration—Applies to the configuration downloaded from the AAA server.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, method lists must be applied to specific lines or interfaces before any of the defined methods will be performed.

The authorization command causes a request packet containing a series of AV pairs to be sent to the RADIUS or TACACS daemon as part of the authorization process. The daemon can do one of the following:

- Accept the request as is.
- Make changes to the request.
- Refuse the request and refuse authorization.

For a list of supported RADIUS attributes, refer to the appendix “RADIUS Attributes” in the *Cisco IOS Security Configuration Guide*. For a list of supported TACACS+ AV pairs, refer to the appendix “TACACS+ Attribute-Value Pairs” in the *Cisco IOS Security Configuration Guide*.

Note Five commands are associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included in the privilege level command set.

Examples

The following example defines the network authorization method list named mygroup, which specifies that RADIUS authorization will be used on serial lines using PPP. If the RADIUS server fails to respond, local network authorization will be performed.

```
aaa authorization network mygroup group radius local
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa group server tacacs+	Groups different TACACS+ server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
tacacs-server host	Specifies a TACACS+ host.

aaa cache profile

To create a named authentication and authorization cache profile group and enter profile map configuration mode, use the **aaa cache profile** command in global configuration mode. To disable a cache profile group, use the **no** form of this command.

aaa cache profile *group-name*

no aaa cache profile *group-name*

Syntax Description

group-name	Text string that specifies an authentication and authorization group. Group names cannot be duplicated.

Command Default

No cache profile groups are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Use this command to define or modify an authentication or authorization cache group.

After enabling this command, you can specify cache profile parameters using the following commands:

- **profile**—Specifies an exact profile match to cache. The profile name must be an exact match to the username being queried by the service authentication or authorization request. This is the recommended format to enter profiles that users want to cache.
- **regexp**—Allows entries to match based on regular expressions. Matching on regular expressions is not recommended for most situations.

  The **any** keyword, which is available under the **regexp** submenu, allows for any unique instance of a AAA Server Response that matches the regular expression to be saved in the cache. The **only** keyword allows for only one instance of a AAA Server Reponse that matches the regular expression to be saved in the cache.
- **all**—Specifies that all authentication and authorization requests are cached. Using the **all** command makes sense for certain service authorization requests, but it should be avoided when dealing with authentication requests.

Entering the **no** form of this command deletes the profile definition and all of its command definitions.

Examples

The following example shows how to create the AAA cache profile group localusers:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa cache profile localusers
```

Related Commands

Command	Description
all	Specifies that all authentication and authorization requests be cached.
profile	Defines or modifies an individual authentication and authorization cache profile.
regexp	Creates an entry in a cache profile group that allows authentication and authorization matches based on a regular expression.

all (profile map configuration)

To specify that all authentication and authorization requests be cached, use the **all** command in profile map configuration mode. To disable the caching of all requests, use the **no** form of this command.

all [**no-auth**]

no all

Syntax Description

no-auth	(Optional) Specifies that authentication is bypassed for this user.

Command Default

No requests are cached.

Command Modes

Profile map configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Use the **all** command to cache all authentication and authorization requests.

Use the **all** command for specific service authorization requests, but it should be avoided when dealing with authentication requests.

Examples

The following example shows how to specify that all authorization requests be cached in the localusers cache profile group. No authentication is performed for these users because the **no-auth** keyword is used.

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa cache profile localusers
Router(config-profile-map)# all no-auth
```

Related Commands

Command	Description
profile	Defines or modifies an individual authentication and authorization cache profile based on an exact username match.
regexp	Creates an entry in a cache profile group that allows authentication and authorization matches based on a regular expression.

cache authentication profile (server group configuration)

To specify a cache authentication profile to use in a named RADIUS or TACACS+ server group, use the **cache authentication profile** command in server group configuration mode. To disable an authentication cache profile, use the **no** form of this command.

cache authentication profile *name*

no cache authentication profile *name*

Syntax Description

name	Name of an authentication cache profile.

Defaults

No authentication cache profile is enabled.

Command Modes

Server group configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Use this command to specify a cache authentication profile for a RADIUS or TACACS+ server group.

Configure the authentication profile prior to applying it to a RADIUS or TACACS+ server group to avoid an error message.

Examples

The following example shows how to specify that authentication responses from a RADIUS server will be cached according to the rules configured in the authentication profile authen-profile:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa group server radius networkauthentications
Router(config-sg-radius)# cache authentication profile authen-profile
```

Related Commands

Command	Description
cache authorization profile	Specifies an authorization cache profile to use in a named RADIUS or TACACS+ server group.

cache authorization profile (server group configuration)

To specify a cache authorization profile to use in a named RADIUS or TACACS+ server group, use the **cache authorization profile** command in server group configuration mode. To disable an authorization cache profile, use the **no** form of this command.

cache authorization profile *name*

no cache authorization profile *name*

Syntax Description

name	Name of a cache authorization profile to apply to either a RADIUS or TACACS+ server group.

Defaults

No authorization cache profile is enabled.

Command Modes

Server group configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Use this command to specify an authorization profile for a RADIUS or TACACS+ server group.

Examples

The following example shows how to specify that authorization responses from a RADIUS server will be cached according to the rules configured in the authorization profile author-profile:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa group server radius authorizations
Router(config-sg-radius)# cache authorization profile author-profile
```

The authorization profile author-profile must be configured prior to applying it to a RADIUS or TACACS+ server group or an error message is generated.

Related Commands

Command	Description
cache authentication profile	Specifies an authentication cache profile to use in a named RADIUS or TACACS+ server group.

cache expiry (server group configuration)

To configure how long cached database profile entries in RADIUS or TACACS+ server groups are stored before they expire, use the **cache expiry** command in server group configuration mode. To reset the expiration time to the default value, use the **no** form of this command.

cache expiry *hours* [**enforce** | **failover**]

no cache expiry

Syntax Description

hours	Length of time, in hours, for a cache database profile entry to expire. Range is from 0 to 2147483647. Default is 24 hours.
enforce	(Optional) Specifies to not use expired entries.
failover	(Optional) Specifies to use an expired entry if all other methods fail.

Defaults

Cache entries expire in 24 hours.

Command Modes

Server group configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Use this command to set the amount of time before a cache entry expires (becomes stale). A stale entry is still useable, but the entry will, by default, revise its record with more updated information.

Examples

The following example shows how to set the expiration time for cache profile entries to 10 days and specify that expired entries cannot be used:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa group server radius networkusers
Router(config-sg-radius)# cache expiry 240 enforce
```

Related Commands

Command	Description
cache authentication profile	Specifies an authentication cache profile to use in a named RADIUS or TACACS+ server group.
cache authorization profile	Specifies an authorization cache profile to use in a named RADIUS or TACACS+ server group.

clear aaa cache group

To clear an individual entry or all entries in the cache, use the **clear aaa cache group** command in privileged EXEC mode.

clear aaa cache group *name* {**profile** *name* | **all**}

Syntax Description

name	Text string representing the name of a cache server group.
profile *name*	Specifies the name of an individual profile entry to clear.
all	Specifies that all profiles in the named cache group are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Use this command to clear cache entries.

Examples

The following example shows how to clear all cache entries in the localusers group:

```
Router# clear aaa cache group localusers all
```

Related Commands

Command	Description
show aaa cache group	Displays all of the cache entries stored by the AAA Auth Cache.

debug aaa cache group

To debug the caching mechanism and ensure that entries are being cached from AAA Server Responses and are being found when queried, use the **debug aaa cache group** command in privileged EXEC mode.

debug aaa cache group

Syntax Description

This command has no arguments or keywords.

Command Default

Debug information for all cached entries is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Use this command to display debug information about cached entries.

Examples

The following example shows how to display debug information about all cached entries:

```
Router# debug aaa cache group
```

Related Commands

Command	Description
clear aaa cache group	Clears an individual entry or all entries in the cache.
show aaa cache group	Displays cache entries stored by the AAA Auth Cache.

profile (profile map configuration)

To define or modify an individual authentication and authorization cache profile, use the **profile** command in profile map configuration mode. To disable a cache profile, use the **no** form of this command.

profile *name* [**no-auth**]

no profile *name*

Syntax Description

name	Text string that is an exact match to an existing username.
no-auth	(Optional) Specifies that authentication is bypassed for this user.

Command Default

No profiles are defined.

Command Modes

Profile map configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Use the **profile** command to define or modify an authentication and authorization cache profile. The *name* argument in this command must be an exact match to a username being queried by an authentication or authorization service request.

Using the **profile** command with the *name* argument, as opposed to using the **regexp** or **all** command, is the recommended way to cache information.

Examples

The following example shows how to define a cache profile, which includes no user authentication, that is part of the localusers cache profile group:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa cache profile localusers
Router(config-profile-map)# profile user101 no auth
```

Related Commands

Command	Description
aaa cache profile	Creates a named authentication and authorization cache profile group.
all	Specifies that all authentication and authorization requests be cached.
regexp	Creates an entry in a cache profile group that allows authentication and authorization matches based on a regular expression.

regexp (profile map configuration)

To create an entry in a cache profile group that allows authentication and authorization matches based on a regular expression, use the **regexp** command in profile map configuration mode. To disable a regular expression entry, use the **no** form of this command.

regexp *matchexpression* {**any** | **only**} [**no-auth**]

no regexp *matchexpression* {**any** | **only**}

Syntax Description

matchexpression	String representing a regular expression on which to match.
any	Specifies that any unique instance of a AAA Server Response that matches the regular expression is saved in cache.
only	Specifies that only one instance of a AAA Server Response that matches the regular expression is saved in cache.
no-auth	(Optional) Specifies that authentication is bypassed for this user.

Command Default

No regular expression entries are defined.

Command Modes

Profile map configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Use this command to create an entry in a cache profile group that matches based on a regular expression, such as .*@abccompany.com or .*@xyznet.com.

Because the number of entries in a regular expression cache profile group could be in the thousands, and validating each request against a regular expression can be time consuming, we do not recommend using regular expression entries in cache profile groups.

Examples

The following example shows how to create an entry in the cache profile group networkusers that authorizes network access to any ABC company user. No authentication is performed for these users because the **no-auth** keyword is used.

```
Router# configure terminal
Router(config)# aaa cache profile networkusers
Router(config-profile-map)# regexp .*@abccompany.com any no-auth
```

Related Commands

Command	Description
profile	Creates an individual authentication and authorization cache profile based on an exact username match.

show aaa cache group

To display all of the cache entries stored by the AAA Auth Cache, use the **show aaa cache group** command in privileged EXEC mode.

show aaa cache group *name*

Syntax Description

name	Text string representing a cache server group.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Usage Guidelines

Use this command to display all cache entries for a specific group.

Examples

The following example shows how to display all cache entries for the group localusers@company.com:

```
Router# show aaa cache group localusers@company.com
```

Related Commands

Command	Description
clear aaa cache group	Clears individual entries or all entries in the cache.
debug aaa cache group	Debugs the caching mechanism and ensures that entries are being cached from AAA Server Responses and are being found when queried.

Feature Information for Implementing Authorization and Authentication Profile Caching

Table 4 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. 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.

Note Table 4 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 4 Feature Information for Implementing Authentication and Authorization Profile Caching

Feature Name	Release	Feature Information
AAA Authorization and Authentication Cache	12.2(28)SB	This feature optimizes network performance and provides a failover mechanism in the event a network RADIUS or TACACS+ server becomes unavailable for any reason.