Security Configuration Commands

Table of Contents

Chapter 1 AAA Configuration Commands

This Chapter describes the commands used for configuring the AAA authentication method. AAA authentication commands can be classified into authentication, authorization, accounting and local account policy configuration commands. Learn more in following sections.

1.1 Authentication Configuration Commands

This section describes the commands for configuring authentication methods. Authentication defines the access right of the users before they are allowed to access the network and network services.

Please refer to "Configuring Authentication" for information on how to use the AAA method to configure the authentication. Please refer to the last part to review the examples configured by the commands in this Chapter.

Authentication Configuration Commands include:

- aaa authentication banner
- aaa authentication fail-message
- aaa authentication username-prompt
- aaa authentication password-prompt
- aaa authentication dot1x
- aaa authentication enable default
- aaa authentication login
- aaa group server
- server
- debug aaa authentication
- enable password
- enable(enter)
- service password-encryption

1.1.1 aaa authentication banner

Syntax

To configure a personal banner, run aaa authentication banner in global mode. To delete a personal banner, run no aaa authentication banner.

aaa authentication banner *delimiter string delimiter*
no aaa authentication banner

Parameters

Parameters	Description
delimiter string delimiter	To-be-displayed text string when the user logs in; The delimiter parameter stands for the delimiter which adopts double quotation masks.

Default Value

If you do not define the login banner, the system will display the following default banner:
User Access Verification

Command Mode

Global configuration mode

Usage Guidelines

When creating a banner, you need to configure a delimiter and then to configure the text string itself. The delimiter is to notify that the following text string will be displayed as the banner. The delimiter appears repeatedly at the end of the string, meaning the banner ends.

Example

The following example shows that the banner is modified to "Welcome to AACOM system" when logging on:
aaa authentication banner "Welcome to   system!"

Related Command

aaa authentication fail-message

1.1.2 aaa authentication fail-message

Syntax

To configure a personal banner when login fails, run aaa authentication fail-message in global mode. To delete a personal banner, use the no form of this command.
aaa authentication fail-message *delimiter string delimiter*
no aaa authentication fail-message

Parameters

Parameters	Description
delimiter string delimiter	Text string that will be displayed when user fails to log in. The delimiter adopts double quotation

	marks.

Default Value

If you do not define the login banner, the system will display the following default banner:
Authentication failed!

Command Mode

Global configuration mode

Usage Guidelines

When creating a banner, you need to configure a delimiter and then to configure the text string itself. The delimiter is to notify that the following text string will be displayed as the banner. The delimiter appears repeatedly at the end of the string, meaning the banner ends.

Example

The following example shows that user name prompt is changed to the following character string:
aaa authentication fail-message "See you later"

Related Command

aaa authentication banner

1.1.3 aaa authentication username-prompt

Syntax

To change the text display prompting the user name input, run command "aaa authentication username-prompt" in global mode. To return to the default setting, use the no form of this command.
aaa authentication username-prompt text-string
no aaa authentication username-prompt

Parameters

Parameters	Description
text-string	It is used to prompt the user of the text to be displayed at the time of the user name input.

Default Value

When there is no user-defined text-string, the prompting character string of the user name is "Username".

Command Mode

Global configuration mode

Usage Guidelines

The command "aaa authentication username-prompt" is used for changing the displayed character string prompting the user name input. The "no" format of the command changes the prompt of username into default value.
Username:
Some protocols (such as TACACS+) have the capability to cover the prompting information of local username. Under such circumstances, the use of the command "aaa authentication username-prompt" will not change the prompting character string of username.
Note:
The command "aaa authentication username-prompt" does not change any prompting information provided by remote TACACS +server.

Example

The following example shows that user name prompt is changed to the following character string:
aaa authentication username-prompt "YourUsername:"

Related Command

aaa authentication password-prompt

1.1.4 aaa authentication password-prompt

Syntax

To change the text display prompting the user password input, run command "aaa authentication password-prompt" in global configuration mode. To return to the default setting, use the no form of this command.
aaa authentication password-prompt *text-string*
no aaa authentication password-prompt

Parameters

Parameters	Description
test-string	It is used to prompt the user of the text displayed at the time of password input.

Default Value

When the user-defined text-string is not used, the password prompt is "Password".

Command Mode

Global configuration mode

Usage Guidelines

The displayed default literal information prompting the user password input can be changed by using the command "aaa authentication password-prompt". The command not only changes the password prompt of the enable password, it also changes the password prompt of login password. The "no" format of the command restores the password prompt to default value.
Password:
The command "aaa authentication password-prompt" does not change any prompting information provided by remote TACACS+ or RADIUS server.

Example

The following Example will change the password prompt to "YourPassword:"
aaa authentication password-prompt "YourPassword:"

Related Command

aaa authentication username-prompt
enable password

1.1.5 aaa authentication dot1x

Syntax

To set do1x access authentication, run command aaa authentication dot1x in global configuration mode. To disable dot1x authentication, use the no form of this command.
aaa authentication dot1x {**default** | *list-name*} *method1* [*method2...*]
no aaa authentication dot1x {**default** | *list-name*}

Parameters

Parameters	Description
Default	It uses the listed authentication method following the parameter as the default authentication method list at the time of the user's login.
list-name	It uses the listed authentication method following the parameter as the default authentication method list at the time of the user's login.
method	It is one of the key words described in the Form 2 at the least.

Command Mode

Global configuration mode

Usage Guidelines

The default list or other naming list created by the command "aaa authentication login" will act on some specific line using the command "login authentication".
Only when the said authentication method feeds back error, other authentication methods will be used. Should the said authentication method feedback the failure, no other authentication methods will be used.

dot1x authentication method

Keyword	Description
group name	Uses the server group for authentication.
group radius	Uses RADIUS authentication.
group tacacs+	Uses group tacacs+ for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local user name authentication.
none	Uses no authentication.

Example

The following example creates an AAA authentication list called TEST. 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. (Now the authentication method either enable(line) or local can obtain a success or failure result. Therefore, the following command will not use the none method.
aaa authentication dot1x TEST group tacacs+ local 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 dot1x default group tacacs+ local none

Related Command

None

1.1.6 aaa authentication enable default

Syntax

To enable AAA authentication to determine if a user can access the privileged command level, use the aaa authentication enable default global configuration command. To disable this authentication method, use the no form of this command.
aaa authentication enable default *method1* [*method2...*]

no aaa authentication enable default

Parameters

Parameters	Description
method	At least one of the keywords described in Table 1.

Default Value

No authentication method is set. The authentication will succeed if it is the console port user. Otherwise, the authentication will fail.

Command Mode

Global configuration mode

Usage Guidelines

Use the aaa authentication enable default command to create a series of authentication methods that are used to determine whether a user can access the privileged command level. Method keywords are described in Table 1. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify none as the final method in the command line.Only when the said authentication method feeds back error, other authentication methods will be used. Should the said authentication method feedback the failure, no other authentication methods will be used.

enable authentication method

Keyword	Description
enable	Uses the enable password for authentication.
group name	Uses the server group for authentication.
group radius	Uses RADIUS authentication.
group tacacs+	Uses tacacs+ for authentication.
line	Uses the line password for authentication.
none	Passes the authentication unconditionally.

Example

The following example creates an authentication list that first tries to contact a TACACS+ server. If no server can be found, 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. (Now the authentication method either enable (line) or local can obtain a success or failure result. Therefore, the following command will not use the none method.

aaa authentication enable default group tacacs+ enable none

Related Command

enable password

1.1.7 aaa authentication login

Syntax

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*}

Parameters

Parameters	Description
Default	Uses the listed authentication methods that follow this argument 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.
method	At least one of the keywords described in Table 2.

Default Value

No authentication method is set. The authentication will succeed if it is the console port user. Otherwise, the authentication will fail.

Command Mode

Global configuration mode

Usage Guidelines

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

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.

login authentication method

Keyword	Description
enable	Uses the enable password for authentication.
group name	Uses the server group for authentication.
group radius	Uses RADIUS authentication.
group tacacs+	Uses group tacacs+ for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
localgroup	Uses the local strategy group username database for authentication.
local-case	Uses case-sensitive local user name authentication.
none	Uses no authentication.

Example

The following example creates an AAA authentication list called TEST. 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 TEST group tacacs+ group radius 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+ group radius none

Related Command

None

1.1.8 aaa group server

Syntax

To group different RADIUS server hosts into distinct lists and distinct methods, run command aaa group server radius in global configuration mode. To remove a group server from the configuration list, use the no form of this command.
aaa group server {radius | tacacs+} *group-name*
no aaa group server {radius | tacacs+} *group-name*

Parameters

Parameters	Description
group-name	Character string used to name the group of servers.

Default Value

No default behavior or values.

Command Mode

Global configuration mode

Usage Guidelines

The command is used to enter the configuration of the server group and add the corresponding server to it. It can establish 63 server groups in maximum.

Example

aaa group server radius radius-group
The example shows how to add a radius server group named radius-group.

Related Command

server

1.1.9 server

Syntax

To add a server in an AAA server group, run the following command. To delete a server, use the no form of this command.
To add a server in a radius server group:
server {A.B.C.D | X:X:X:X::X} [**key** {*password* | {*encryption-type encrypted-password*}}] [**auth-port** *num*] [**acct-port** *num*] [**retransmit** *value*] [**timeout** *value*] [**privilege** *pri*]
To add a server to a tacacs+ server group:
server {A.B.C.D | X:X:X:X::X} [**key** {*password* | {*encryption-type encrypted-password*}}]
no server A.B.C.D

Parameters

Parameters	Description
A.B.C.D	IP address of the server
X:X:X:X::X	IPv6 address of the server
key	Key
password	key character string
encryption-type	encryption type, 0 means no encryption, and 7 means encryption.
encrypted-password	key character string corresponding to the encryption type
auth-port	authentication destination port
acct-port	accounting destination port
num	Standing for a port ID
retransmit *value*	retransmit times, the default is 2.
timeout *value*	timeout for retransmit. The default is 3 seconds.
privilege *pri*	server priority; the default is 0.

Default Value

no server

Command Mode

Server group configuration mode

Usage Guidelines

You can add 63 server groups at most,1 radius server link table and 1 tacacs+ server link table. The value of all radius server groups and servers in the server link table amounts to 64. The value of all tacacs+ server groups and servers in the server link table also amounts to 64.

Example

The following example adds a server at 12.1.1.1 to the server group:
server 12.1.1.1

Related Command

aaa group server

1.1.10 debug aaa authentication

Syntax

To track the user authentication process, run debug aaa authentication. To disable the debug information, run no debug aaa authentication.
debug aaa authentication
no debug aaa authentication

Parameters

None

Default Value

The debug information is disabled by default.

Command Mode

EXEC

Usage Guidelines

This command can be used to track the authentication process of each user to detect the cause of the authentication failure.

Example

None

Related Command

None

1.1.11 enable password

Syntax

To set a local password to control access to various privilege levels, use the enable password command. To remove the password requirement, use the no form of this command.
enable password { *password* | [*encryption-type*] *encrypted-password* } [**level** *number*]
no enable password [**level** *number*]

Parameters

Parameters	Description
password	Plain text of the password character string
encryption-type	Type of password encryption
encrypted-password	Encrypted password corresponding to the set encryption type
level	Privilege level parameter
number	Value of the privilege level (1-15)

Default Value

There is no password by default.

Command Mode

Global configuration mode

Usage Guidelines

The passwords configured for the device do not contain space, that is, when the enable password command is used, space cannot be entered when you enter the plain text of the password. The length of the password plain-text cannot exceed 127 characters.

When the level parameter is not entered, the default level is level 15. The higher the privilege level is, the more rights the user has. If some privilege level is not configured with password, authentication will fail when the user enters the level.

Currently, our products only support two encryption modes: 0 and 7. The number 0 means the password is not encrypted and the plaintext of password is directly entered. It is the same as the way of directly entering the password. The number 7 means the password is encrypted through an algorithm. You need to enter the encryption text for the encrypted password. The encryption text

can be copied from the configuration files of other switches.

Example

The following example shows how to set the password of privilege level 10 to clever and encryption-type to 0.

enable password 0 clever level 10

The following example shows how to set the password of the default privilege level (15) to oscar and encryption-type to 7.

enable password 7 074A05190326

Suppose that the cipher text of oscar is 074A05190326, the value of the cipher text is obtained from the configuration files of other devices.

Related Command

aaa authentication enable default
service password-encryption

1.1.12 enable(enter)

Syntax

To enter the privilege mode (EXEC mode), run command enable(enter).

enable(enter) *<1-15>*

Parameters

Parameters	Description
<1-15>	To be obtained privilege level

Default Value

Do not enter the privileged level by default.

Command Mode

User mode

Usage Guidelines

None

Example

>enable(The user level is 15 by default.)
Password: (enter the password to authenticate)
#

#exi
>enable 1(To be obtained privilege level is 1)
Password: (enter the password to authenticate)
#

Related Command

aaa authentication enable default
enable password

1.1.13 service password-encryption

Syntax

To encrypt passwords, use the service password-encryption command. To return to the default setting, use the no form of this command.
service password-encryption
no service password-encryption

Parameters

None

Default Value

Related passwords in the system are not encrypted.

Command Mode

Global configuration mode

Usage Guidelines

This command is related with three commands, username password, enable password and password. If this command is not configured and the previous three commands adopt the password plain-text storage mode, the configured password's plain text can be displayed after the show running-config command is run. If this command is configured, the passwords configured for the previous three commands will be encrypted and the configured password's plain text cannot be displayed after the show running-config command is run; in this case, the password plain-text display cannot be resumed even if you run no service password-encryption. The no service password-encryption command is effective only to the password which is configured by this command, while is not effective to those passwords which are encrypted before this command is used.

Example

switch_config#service password-encryption
The example show how to encrypt the configured plain-text password and also the plain-text password after this command is used.

Related Command

username username **password**
enable password
password (the configuration command under vty which can be used for line authentication)

1.2 Authorization Configuration Commands

This chapter describes the commands for authentication, authorization and accounting. AAA authorization can limit the effective service to a user. When the authorization result is effective, network access server configures the dialogue process of the user by using the authorization information fed back from authorization server. Then the user is available to services required. Only information included in the user profile provides such service.
Please refer to "Configuration Authorization" for information on how to configure authorization. Please refer to the last part to review the examples configured by the commands in this Chapter.
Authorization Configuration Commands include:
aaa authorization
debug aaa authorization

1.2.1 aaa authorization

Syntax

The global configuration command "aaa authorization" is used for setting the parameter to limit the authority of the user's access to network.
To set the parameter to limit the authority of the user's access to network, run command "aaa authorization" in global configuration mode. To return to the default setting, use the no form of this command.
aaa authorization {{commands *<0-15>***} | network** | **exec}** {**default** | *list-name*} *method1* [*method2...*]
no aaa authorization {{commands *<0-15>*} | network **|** exec } **{**default **|** *list-name***}**

Parameters

Parameters	Description
commands	EXEC（shell）command authorization
<0-15>	To be authorized command privilege (EXEC)
network	The authorization of network type service

exec	It adapts to the attribute related to the user EXEC terminal dialogue. It determines whether XEC shell program is allowed to register or grant the privilege level of the user entering EXEC shell.
default	Default authorization methods list
list-name	Character string which is used to name the authorization method list
method	At least one of the keywords listed in the form below.

Default Value

If the user requires accounting but he does not designate the authorization method list on the corresponding path or interface, the default authorization method list will be applied. If the default method list is not defined, the authorization will not be executed.

Command Mode

Global configuration mode

Usage Guidelines

The command "aaa authorization" is used for enabling the authorization, creating authorization methods list and defining the authorization method that can be used when the user accesses to the designated functions. The authorization method list defines the authorization execution method and the order to execute these authorization methods. The method list is just a simple naming list, describing the authorization method (RADIUS or TACACS+). The method list can designate one or multiple authorization security protocols. Hence, it secures a standby method if all previous authorization methods fail.   Under general condition, the listed first method is used at first in an attempt to authorize the user the authority to access to the designated network service. If the method does not work, the next method in the list shall be selected. The process shall be continued till the successful feedback of authorization results by using some authorization method or all the defined methods are used up.

Authorization method

Keyword	Description
group name	Uses the server group for authorization.
group radius	Uses RADIUS authorization.
group tacacs+	Uses tacacs+ authorization.
if-authenticated	If the user passes the authorization, the user is allowed to access the function required.
local	The local database is used for authorization.
none	No authorization

Once the authorization methods list is defined, the methods list shall be used on the designated line or interface before the defined method is executed. As a part of the authorization process, the authorization command sends a series of request packets of AV pairs to the program of RADIUS or TACACS＋server. The server is likely to execute one of the following actions:

- The request is accepted completely.
- The request is accepted and the attribute is added to limit the authority of user

    service.

- Request is refused and authorization fails.

Example

The following Example defines the network authorization methods list named "have a try". The methods list designates RADIUS authorization method used on the serial line employing vty. If RADIUS server makes no response, the local network authorization is executed.
aaa authorization exec have_a_try radius local
    Related Command
aaa authentication
aaa accounting

1.2.2 debug aaa authorization

Syntax

To track the user authorization process, run debug aaa authorization command. To disable the debug information, run the no form of this command.
debug aaa authorization
no debug aaa authorization

Parameters

None

Default Value

The debug information is disabled by default.

Command Mode

EXEC

Usage Guidelines

This command can be used to track the authorization process of each user to detect the cause of the authorization failure.

Example

None

Related Command

None

1.3 Accounting Configuration Commands

This chapter describes the commands for accounting. The accounting function can track the services that users access, and at the same time track the service-consumed network resource number. When AAA accounting is activated, the system will report user's activities to the TACACS+ server or the RADIUS server in the accounting record method (It depends on the adopted security method). Each accounting record contains the attribute value peer which is stored on the access control server. The data is then applied to network management, client's accounting analysis or audit.

Authorization Configuration Commands include:

- aaa accounting
- aaa accounting update
- aaa accounting suppress null-username
- debug aaa accounting

1.3.1 aaa accounting

Syntax

To execute AAA accounting onto required services on the basis of accounting or security, run aaa accounting in global mode. You can run no aaa accounting to disable the accounting function.

aaa accounting {{**commands** *<0-15>*} **| network** | **exec** | **connection**} {**default** | *list-name*} {{{**start-stop** | **stop-only**} **group** {*groupname* | **radius | tacacs+**}} | **none** }

no aaa accounting **{** network **|** exec **|** connection**} {**default **|** *list-name***}**

Parameters

Parameters	Description
commands	Provide accounting for a priority level command
<0-15>	The priority level of the command
network	Provides accounting information to all PPP sessions, including packets, bytes and time numbering.
exec	Provides information about EXEC terminal session (it is not supported currently).
connection	Provides information about all egress connections from related device. Currently, only the H323 session is supported.
default	Default accounting method list
list-name	Character string which is used to name the accounting method list
start-stop	accounting in beginning and end
stop-only	accounting in the end
none	no accounting

group *groupname*	Uses the server group for accounting
group radius	Uses RADIUS for accounting
group tacacs+	Uses tacacs+ for accounting

Default Value

If the user requires accounting but he does not designate the accounting method list on the corresponding path or interface, the default accounting method list will be applied. If the default method list is not defined, the accounting will not be executed.

Command Mode

Global configuration mode

Usage Guidelines

You can use the aaa accounting command to enable the accounting function, create the accounting method list and define the applied accounting method when user sends the accounting record. The accounting method list defines the accounting execution method and the order to execute these accounting methods. The method list is just a simple naming list, describing the accounting method (RADIUS or TACACS+). The method list can designate one or multiple accounting security protocols. Hence, it secures a standby method if all previous accounting methods fail.

Related Command

aaa authentication
aaa accounting

1.3.2 aaa accounting update

Syntax

To periodically transmit temporary accounting records to the accounting server, run aaa accounting update. You can run no aaa accounting update to disable temporary accounting records.

aaa accounting update { **newinfo** | **periodic** *number*}

no aaa accounting update **{** newinfo **|** periodic**}**

Parameters

Parameters	Description
update	Activates the device to transmit temporary accounting records (It needs support from the application client. It is not supported at present.).
newinfo	Transmits temporary accounting records to the accounting

	server when new accounting information need be reported.
periodic	Periodically transmits temporary accounting records. The period is defined by the number parameter.
number	A parameter to define the period for temporary accounting record transmission

Default Value

Temporary accounting activity does not occur.

Command Mode

Global configuration mode

Usage Guidelines

The function runs with the support of the application client. It is not supported at present.

Related Command

aaa accounting

1.3.3 aaa accounting suppress null-username

Syntax

To stop generating accounting records for those non-user sessions, run aaa accounting suppress null-username in global mode. To return to the default setting, use the no form of this command.

aaa accounting suppress null-username
no aaa accounting suppress null-username

Parameters

None

Default Value

The accounting records will be generated for all sessions, no matter the sessions have username or not.

Command Mode

Global configuration mode

Usage Guidelines

None

Related Command

aaa accounting

1.3.4 debug aaa accounting

Syntax

To track the user accouting process, run debug aaa accouting command. To disable the debug information, run the no form of this command.

debug aaa accounting

no debug aaa accounting

Parameters

None

Default Value

The debug information is disabled by default.

Command Mode

EXEC

Usage Guidelines

This command can be used to track the accounting process of each user to detect the cause of the accounting failure.

Example

None

Related Command

None

1.4 Local Account Policy Configuration Commands

This section introduces local account policy configuration commands. The local account policy is used for local authentication and local authorization.

Please refer to "local account policy configuration" for information on how to configure local account policy. Please refer to the last part to review the examples configured by the commands in this Chapter.

Local Account Policy Configuration Commands include:

localauthen

localauthor

localpass

localgroup

local authen-group

local author-group

local pass-group

local user

username

show local-users

show aaa users

1.4.1 localauthen

Syntax

To configure local authentication policy, run the command localauthen. To return to the default setting, use the no form of this command.

localauthen **WORD**

no localauthen **WORD**

Parameters

Parameters	Description
WORD	Local authentication policy name

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

To enter local authentication configuration, run command localauthen WORD.

The max login tries within a certain time

login max-tries *<1-9>* **try-duration** *1d2h3m4s*

Parameters	Description
max-tries	The max login tries
<1-9>	The max login tries ranges from 1 to 9
try-duration	Duration
1d2h3m4s	The format of day, hour, min and second.

Related Command

login max-tries
localgroup
local authen-group
username

1.4.2 localauthor

Syntax

To configure local authentication policy, run the command localauthen. To return to the default setting, use the no form of this command.

localauthor *WORD*

no localauthen *WORD*

Parameters

Parameters	Description
WORD	Local authorization policy name

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command localauthor WORD is used to enter the local authorization policy configuration. Use following command to configure local authorization policy.

To authorize priority for login users.

exec privilege {**default | console | ssh | telnet}** *<1-15>*

Parameters	Description
default	Default priority (Use the priority for authorization if there is no concrete login method.)
console	authorization priority of the login user on console port
ssh	authorization priority of the ssh login user on console port
telnet	authorization priority of the telnet login user on console port
<1-15>	Priority

Related Command

exec privilege
localgroup
local author-group
username

1.4.3 localpass

Syntax

To configure local password policy, run the command localpass in global mode. To return to the default setting, use the no form of this command.
localpass *WORD*
no localpass *WORD*

Parameters

Parameters	Description
WORD	Local password policy name

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command localpass WORD is used to enter the local password policy configuration. Use following command to configure local password policy.
The password and username is different
     non-user
History password check (When the password is different from the history one or modifying the password)
     non-history
Set the elements of the password
     element *[number] [lower-letter] [upper-letter] [special-character]*

Parameters	Description
number	The password must include numbers.
lower-letter	The password must include lower-letters.
upper-letter	The password must include upper-letters.
special-character	The password must include special characters.

The minimum length of the password

min-length *<1-127>*

Parameters	Description
<1-127>	The minimum length (ranges from 1-127)

The validity of the password

validity *1d2h3m4s*

Parameters	Description
1d2h3m4s	The format of day, hour, min and second.

Related Command

non-use

non-history

element

min-length

validity

localgroup

local pass-group

username

1.4.4 localgroup

Syntax

To configure local policy group, run command localgroup in global mode. To return to the default setting, use the no form of this command.

localgroup *WORD*

no localgroup *WORD*

Parameters

Parameters	Description
WORD	Local policy group name

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command localgroup WORD is used to enter the local password policy configuration. Use following command to configure local policy group.
Stands for the local authentication configuration
local authen-group
Stands for the local authorization configuration
local author-group
Local password configuration
local pass-group
Local account configuration
local user
Configuring account
username

Related Command

local authen-group
local author-group
local pass-group
local user
username
localgroup
local author-group

1.4.5 local authen-group

Syntax

To configure local authentication policy group, run command local authen-group. It is local policy group in global mode by default. To return to the default setting, use the no form of this command.
local authen-group *WORD*
no local authen-group

Parameters

Parameters	Description
WORD	Local authentication policy name

Default Value

None

Command Mode

Global configuration mode, local policy group configuration mode

Usage Guidelines

None

Related Command

localauthen
localgroup
local authen-group

1.4.6 local author-group

Syntax

To configure local authentication policy group, run command local author-group. It is the local policy group in global mode by default. To return to the default setting, use the no form of this command.
local author-group *WORD*
no local author-group

Parameters

Parameters	Description
WORD	Local authorization policy name

Default Value

None

Command Mode

Global configuration mode, local policy group configuration mode

Usage Guidelines

None

Related Command

localauthor
localgroup
local author-group

1.4.7 local pass-group

Syntax

To configure local password policy group, run command local pass-group. It is the default policy group by default in global configuration mode. To return to the default setting, use the no form of this command.

local pass-group *WORD*

no local pass-group

Parameters

Parameters	Description
WORD	Local password policy name

Default Value

None

Command Mode

Global configuration mode, local policy group configuration mode

Usage Guidelines

None

Related Command

localpass
localgroup
local pass-group

1.4.8 local user

Syntax

To configure the maximum connection numbers and freezing users, run command local user. It is the default policy group by default in global configuration mode. To return to the default setting, use the no form of this command.

local user {maxlinks *<1-255>***} | {** **freeze** *WORD* **}**

no local user {maxlinks **| {** freeze *WORD* **}}**

Parameters

Parameters	Description
maxlinks	The maximum links to the router, the same user can create at the same time.
<1-255>	The number of links created at the same time. (value range: 1-255)
freeze	freezing user
WORD	A user name

Default Value

None

Command Mode

Global configuration mode, local policy group configuration mode

Usage Guidelines

None

Related Command

localgroup

1.4.9 username

Syntax

To add users in the local user database for local authentication and authorization, run this command. The command is used in local policy group configuration mode. It is the default local policy group in global configuration mode. To return to the default setting, use the no form of this command.

username *username* [**password** *password* **|** {encryption-type *encrypted-password*}] [**maxlinks** *number*] [**authen-group** *WORD*] [**author-group** *WORD*] [**pass-group** *WORD*] [**autocommand** *command*] [**bind-ip** *A.B.C.D*] [**bind-mac** *H:H:H:H:H:H*] [**bind-pool** *WORD*] [**bind-port** *port*][**callback-dialstring** *string*] [**callback-line** *line*] [**callback-rotary** *rotary*] [**nocallback-verify**] [**nohangup**] [**noescape**]

no username *username*

Parameters

Parameters	Description
username	Character string of username
password	User password
password	Plain text of the password character string
encryption-type	Type of password encryption

encrypted-password	Cipher text of the password which corresponds to the limited encryption type
maxlinks	The maximum links to the device, the same user can create at the same time
number	number of links
authen-group	*Set the local authentication policy*
WORD	Local authentication policy name
author-group	*Set the local authorization policy*
WORD	Local authorization policy name
pass-group	*Set the local password policy*
WORD	Local password policy name
autocommand	Run the specified command when the user logs in. autocommand must run at the end of the command line.
command	Run the command character string automatically.
The switch does not support following options.	
bind-ip	*bind user IP address (non-support)*
A.B.C.D	IP address
bind-mac	*bind user mac address (non-support)*
H:H:H:H:H:H	*48 byte hardware address of ARP record*
bind-pool	*bind user address pool (non-support)*
WORD	address pool name
bind-port	*bind user port (non-support)*
Port	Port
callback-dialstring	callback dial (non-support)
string	telephone number character string
callback-line	callback line (non-support)
line	Stands for the ID of the line.
callback-rotary	callback rotary configuration (non-support)
rotary	rotary number;
nocallback-verify :	no callback verify (non-support)
nohangup	no hangup after the user logs in and run the command automatically (non-support)
noescape	no escape character after the user logs in (non-support)

Default Value

no users

Command Mode

Global configuration mode, local policy group configuration mode

Usage Guidelines

The password is considered as empty character string when there is no password parameter.
user-maxlinks limits the session numbers the same account can establish. But the account will not
be counts in if its session is not authenticated by local authentication. Command show aaa users
can be used to check the basic information of each on-line user.
The passwords configured for the device do not contain space, that is, when the enable password
command is used, space cannot be entered when you enter the plain text of the password.
Currently, our products only support two encryption modes: 0 and 7. The number 0 means the

password is not encrypted and the plaintext of password is directly entered. It is the same as the way of directly entering the password. The number 7 means the password is encrypted through an algorithm . You need to enter the encryption text for the encrypted password. The encryption text can be copied from the configuration files of other switches.

Example

The local user is added in the Example below. The username is someone, the password is someother.

username someone password someother

The local user is added in the Example below, the username is Oscar, the password is Joan. The encryption type applied is 7, namely the encryption method, the ciphertext of the password is needed to be entered.

enable password 7 1105718265

Given the assumption that the ciphertext of Joan is 1105718265, the value of the ciphertext is obtained from the configuration files of other routers.

Related Command

aaa authentication login

1.4.10 show local-users

Syntax

To show summary informationn of all local AAA account, run command show local-users.
show local-users

Parameters

None

Default Value

None

Command Mode

EXEC

Usage Guidelines

The command is used to show all AAA accounts, including following information: Local group default, links, pw_present, login_tries, login_try_time, and freezing_cause.

Example

#show local-users
Local group default:

username	links	pw_present	login_tries	login_try_time	freezing_cause
admin	1	0s	0	0s	
aaa	0	0s	0	0s	

Domain	Description
Local group default:	The local policy group that the accout belongs to
links	The connections that the account is using (repesents how much users are using the accout.)
pw_present	Password validity period
login_tries	login password failure times (sets the maximum failure times and 0 means no set)
login_try_time	login password failure time (sets the maximum failure times and 0 means no set)
freezing_cause	reason of the account being frozen

Related Command

username

1.4.11 show aaa users

Syntax

To display the summary information about all online AAA users, run show aaa users.
show aaa users

Parameters

None

Default Value

None

Command Mode

EXEC

Usage Guidelines

After this command is run, the following information about online users can be displayed: port, username, service, online duration time and peer_address.

Example

#show aaa users

Port	User	Service	Duration	Peer Address

===

console 0   zjl   exec   04:14:03   unknown

vty 0   aaa   exec   00:12:24   172.16.20.120

Domain	Description
Port	ID of the interface where user lies, or index number of VTY
User	Character string of username
Service	Service applied by the user
Duration	Online duration time of the user
Peer Address	IP address of the remote host where the user lies

Related Command

username

Chapter 2 RADIUS Configuration Commands

This chapter introduces the commands for RADIUS configuration. RADIUS is a distributed client/server system capable of denying the unauthorized network access. RADIUS client is running on the router and sends the request of authentication, authorization and accounting to the central RADIUS server containing the authentication of all the user and the information of network service access.

Please refer to "RADIUS Configuration" about how to configure RADIUS information and learn more about configuration examples.

2.1 RADIUS Configuration Commands

RADIUS Configuration commands include:
- debug radius
- ip radius source-interface
- radius-server challenge-noecho
- radius-server deadtime
- radius-server host
- radius-server key
- radius-server optional-passwords
- radius-server retransmit
- radius-server timeout
- radius-server vsa send
- radius-server attribute
- radius-server directed-resquest

2.1.1 debug radius

Syntax

To track RADIUS event or packet, run command debug radius. To disable the debug information, run the no form of this command.

debug radius ｛*event | packet*｝
no debug radius ｛*event | packet*｝

Parameters

Parameters	Description
event	Tracing RADIUS event.
packet	Tracing RADIUS packets.

Default Value

None

Command Mode

EXEC

Usage Guidelines

The command can be used for network system debug and finding the reason of user authentication failure.

Example

The following example shows how to enable RADIUS event track:
debug radius event

2.1.2 ip radius source-interface

Syntax

To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the ip radius source-interface command in global configuration mode. To prevent RADIUS from using the IP address of a specified interface for all outgoing RADIUS packets, use the no form of this command.
ip radius source-interface *interface-name*
no ip radius source-interface

Parameters

Parameters	Description
interface-name	Name of the interface that RADIUS uses for all of its outgoing packets.

Default Value

No default behavior or values

Command Mode

Global configuration mode

Usage Guidelines

Use this command to set the IP address of a subinterface to be used as the source address for all outgoing RADIUS packets. The IP address is used as long as the subinterface is in the up state. In this way, the RADIUS server can use one IP address entry for every network access client instead

of maintaining a list of IP addresses. This command is especially useful in cases where the device has many subinterfaces and you want to ensure that all RADIUS packets from a particular device have the same IP address.

The specified subinterface must have an IP address associated with it. If the specified subinterface does not have an IP address or is in the down state, then RADIUS reverts to the default. To avoid this, add an IP address to the subinterface or bring the subinterface to the up state.

Example

The following example shows how to configure RADIUS to use the IP address of vlan 1 for all outgoing RADIUS packets:
ip radius source-interface vlan 1

Related Command

ip tacacs source-interface

2.1.3 radius-server attribute

Syntax

To designate some attributes to be transmitted during radius authentication and charging, run radius-server attribute. To disable AAA authentication, use the no form of this command.
radius-server attribute {**4** | **32** | **95**}
no radius-server attribute {**4** | **32** | **95**}

Parameters

Parameters	Description
4	Transmits the following address as attribute 4 (NAS ip address) during radius operation.
32	Transmits attribute 32 (NAS identifier) during radius authentication or request.
95	Transmits the following address as attribute 95 (NAS ipv6 address) during radius operation.

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

This command is used to designate a specific attribute to be transmitted during radius

36

authentication or radius request.

The radius-server attribute 4 command is used to configure attribute 4 (NAS ip address) in radius and transmit it in the RADIUS packets.

The radius-server attribute 32 command is used to designate attribute 32 (NAS ID) to be transmitted in Radius authentication or charging.

The radius-server attribute 95 command is used to configure attribute 95 (NAS ipv6 address) in radius and transmit it in the RADIUS packets.

Example

The radius-server attribute 4 X.X.X.X command is used when attribute 4 need be transmitted in the Radius packets and attribute 4 serves as the attribute value of X.X.X.X.

The radius-server attribute 32 in-access-req command is used when the NAS identifier need be transmitted in the authentication request.

The radius-server attribute 32 in-account-req command is used when the NAS identifier need be transmitted in the charging request.

radius-server attribute 32 *identifier* configuring NAS identifier

The radius-server attribute 95 X:X:X:X::X command is used when attribute 95 need be transmitted in the Radius packets and X:X:X:X::X serves as the attribute value.

Related Command

None

2.1.4 radius-server challenge-noecho

Syntax

The command "radius-server challenge-noecho" shall be used for not showing the user data under the Access-Challenge Mode.

radius-server challenge-noecho
no radius-server challenge-noecho

Parameters

None

Default Value

The user data is shown under the Access-Challenge.

Command Mode

Global configuration mode

Usage Guidelines

None

Example

radius-server challenge-noecho

2.1.5 radius-server deadtime

Syntax

The global configuration command "radius-server dead-time" shall be used for improving the echo time of RADIUS when some servers are not workable. The command allows the system to skip the unworkable servers. The "no" format of the command can be used for setting dead-time as 0, namely, all the servers are thought to be workable.

radius-server deadtime *minutes*

no radius-server deadtime

Parameters

Parameters	Description
minutes	The time length of RADIUS server thought to be unworkable, the maximum length is 1440 minutes (24 hours)

Default Value

The unworkable time is set as 0, meaning that the server is thought to be workable all the time.

Command Mode

Global configuration mode

Usage Guidelines

The command is used for labeling those RADIUS servers that do not respond to the authentication request as "dead", which avoids too long waiting for the response before using the next server. The RADIUS server labeled as "dead" is skipped by all the requests during the set minutes unless otherwise all the servers are labeled as "dead".

Example

The following Example designates 5-minute dead time for the RADIUS server that does not respond to the request.

radius-server deadtime 5

Related Command

radius-server host
radius-server retransmit
radius-server timeout

2.1.6 radius-server directed-resquest

Syntax

To enable the user to set RADIUS server with the format of '@server', run command radius-server directed-resquest in global mode. To return to the default setting, use the no form of this command.

radius-server directed-resquest [restricted]
no radius-server directed-resquest [restricted]

Parameters

Parameters	Description
restricted	The user can only use the format of '@server' to set RADIUS server.

Default Value

It does not support using the format of '@server' to set RADIUS server.

Command Mode

Global configuration mode

Usage Guidelines

None

Example

radius-server directed-resquest

Related Command

None

2.1.7 radius-server host

Syntax

The global configuration command "radius-server host" is used for designating IP address of radius server. The "no" format of the command is used for deleting the designated RADIUS host.

radius-server host *ip-address|ipv6-address* [*auth-port port-number1*] [acct-port *port-number2*]

no radius-server host ip-address|*ipv6-address*

Parameters

Parameters	Description
ip-address	the ip address of RADIUS server
ipv6-address	the IPv6 address of RADIUS server
auth-port	(optional item) Designating UDP destination port for authentication request.
port-number1	(optional item) The port number of authentication request.
acct-port	(optional item) Designating UDP destination port for accounting request.
port-number2	(optional item) The port number of accounting request.

Default Value

Any RADIUS host is not designated.

Command Mode

Global configuration mode

Usage Guidelines

The command "radius server" can be used repeatedly for designating multiple servers. The polling can be made under the order of configuration when necessary.

Example

The Example below designates RADIUS host whose IP address is 1.1.1.1. The default port is used for accounting and authentication.

radius-server host 1.1.1.1

The following Example designates Port 12 as the destination port of authentication request on the RADIUS host whose IP address is 1.2.1.2. Port 16 is used as the destination port of accounting request.

radius-server host 1.2.1.2 auth-port 12 acct-port 16

Related Command

aaa authentication
radius-server key
tacacs server
username

2.1.8 radius-server key

Syntax

The global configuration command shall be used for setting encryption key for RADIUS communication between the router and RADIUS server. The "no" format of command can be used for invalidating the encryption key.

radius-server key *string* | {encryption-type encrypted-password}
no radius-server key

Parameters

Parameters	Description
string	The secret key used for encrypting. The secret key shall match with the one used by RADIUS server.
encryption-type	encryption type, 0 means no encryption, and 7 means encryption.
encrypted-password	The ciphertext of the password corresponding to the encryption type limited by "encryption-type".

Default Value

The key is empty character string.

Command Mode

Global configuration mode.

Usage Guidelines

The key must correspond to the key used by RADIUS server. All start empty blank will be ignored. The key cannot include the empty character.

Example

The following example shows how to set encryption key to "firsttime":
radius-server key firstime

Related Command

radius-server host
tacacs server
username

2.1.9 radius-server optional-passwords

Syntax

To specify that the first RADIUS request to a RADIUS server be made without password verification, use the radius-server optional-passwords command in global configuration mode. To return the default setting, use the no form of this command.
radius-server optional-passwords
no radius-server optional-passwords

Parameters

The command has no parameters or keywords.

Default Value

optional-password is not used by default.

Command Mode

Global configuration mode

Usage Guidelines

When the user enters the login name, the login request is transmitted with the name and a zero-length password. If accepted, the login procedure completes. If the RADIUS server refuses this request, the server software prompts for a password and tries again when the user supplies a password. The RADIUS server must support authentication for users without passwords to make use of this feature.

Example

The following example configures the first login to not require RADIUS verification:
radius-server optional-passwords

Related Command

radius-server host

2.1.10 radius-server retransmit

Syntax

To specify the number of times the software searches the list of RADIUS server hosts before giving up, use the radius-server retransmit command in global configuration mode. To disable retransmission, use the no form of this command.

radius-server retransmit *retries*

no radius-server retransmit

Parameters

Parameters	Description
retries	Maximum number of retransmission attempts. The default is 2 attempts.

Default Value

2 attempts

Command Mode

Global configuration mode

Usage Guidelines

This command is generally used with the radius-server timeout command, indicating the interval for which a router waits for a server host to reply before timing out and the times of retry after timing out.

Example

The following example specifies a retransmit counter value of five times:

radius-server retransmit 5

Related Command

radius-server timeout

2.1.11 radius-server timeout

Syntax

To set the interval for which a router waits for a server host to reply, use the radius-server timeout command in global configuration mode. To return the default setting, use the no form of this

command.
radius-server timeout *seconds*
no radius-server timeout

Parameters

Parameters	Description
seconds	Number that specifies the timeout interval, in seconds. The default is 5 seconds.

Default Value

3 seconds

Command Mode

Global configuration mode

Usage Guidelines

This command is generally used with the radius-server retransmit command.

Example

The following example shows how to set the number of seconds a router waits for a server host to reply before timing out.
radius-server timeout 10

Related Command

None

2.1.12 radius-server vsa send

Syntax

To configure the network access server to recognize and use vendor-specific attributes, use the command radius-server vsa send. To return to the default setting, use the no form of this command.
radius-server vsa send [**authentication**]
no radius-server vsa send [**authentication**]

Parameters

Parameters	Description

authentication	(Optional) Limits the set of recognized vendor-specific attributes to only authentication attributes.

Default Value

Disabled

Command Mode

Global configuration mode

Usage Guidelines

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The radius-server vsa send command enables the network access server to recognize and use both accounting and authentication vendor-specific attributes. Use the authentication keyword with the radius-server vsa send command to limit the set of recognized vendor-specific attributes to just authentication attributes.

Example

The following example configures the network access server to recognize and use vendor-specific accounting attributes:
radius-server vsa send authentication

Related Command

radius-server host

Chapter 3 TACACS+ Configuration Commands

This chapter describes the commands for configuring TACACS+ security protocols. TACACS+ can be used for authenticating the identity of the user, authorization of service authority and the accounting of the execution process of user service.

Please refer to "TACACS+ Configuration" about how to configure TACACS+ information and learn more about configuration examples.

3.1 TACACS+ Configuration Commands

TACACS+ configuration commands include:
- debug tacacs
- ip tacacs source-interface
- tacacs-server host
- tacacs-server key
- tacacs-server timeout

3.1.1 debug tacacs

Syntax

To trace TACACS+protocol event or checking the packets received or sent, run command "debug tacacs". To return to the default setting, use the no form of this command.

debug tacacs {**event** | **packet**}
no debug tacacs {**event** | **packet**}

Parameters

Parameters	Description
event	Tracing TACACS+ event
packet	Tracing TACACS+ packet

Default Value

The debug information is disabled by default.

Command Mode

EXEC

Usage Guidelines

The command is only used for the debugging of the network to find out the cause of failure of AAA service.

Example

The following example shows how the debugging of the network to find out the cause of failure of AAA service.
debug tacacs event

Related Command

None

3.1.2 ip tacacs source-interface

Syntax

To apply IP address of the designated interface to all the TACACS＋ packets, run command "ip tacacs source-interface" in global mode. To return to the default setting, use the no form of this command.
ip tacacs source-interface *subinterface-name*
no ip tacacs source-interface

Parameters

Parameters	Description
subinterface-name	Interface name corresponding to the source IP address of all TACACS＋ packets.

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command can be used to set source IP address for all TACACS＋ packets by designating the source interface. So long as the interface is under "up" state, all TACACS+ packets will use IP address of the interface as the source address, thus ensuring that TACACS+ packet of each router will have the same source IP address. So TACACS＋ server will not need to maintain the address list containing the IP address. That is to say, in order to ensure all TACACS＋ packets

coming from the specific router to have the same source IP address, the command will work when the router has many interfaces.

The designated interface shall have the IP address linked to the interface. If the designated interface has no IP address or is under a "down" state, the default value will be restored, namely the source IP address shall be determined on the real condition. In order to avoid the case, the IP address shall be added to the interface and the interface shall be ensured under the "up" state.

Example

The following Example will use IP address of the interface vlan1 as source IP address of all TACACS+ packets.
ip tacacs source-interface vlan1

Related Command

ip radius source-interface

3.1.3 tacacs-server host

Syntax

To designate TACACS+ server in global configuration mode, run command "tacacs server host". To return to the default setting, use the no form of this command.
tacacs-server host *ip-address*　[**single-connection**|**multi-connection**] [**port** *integer1*] [**timeout** *integer2*] [**key** *string*]
no tacacs-serve *ip-address*

Parameters

Parameters	Description
ip-address	IP address of the server
single-connection	(optional) Designating router to maintain the single and open TCP connection for the confirmation from AAA/TACACS+ server.
multi-connection	(Optional) Designating router to maintain the different TCP connection for the different confirmation from AAA/TACACS+ server
Port	(optional) Designating port number of server. The option covers the default port number 49.
integer1	(optional) The port number of server. The range of valid port number is 1 to 65536.
timeout	(optional) Designating the timeout of waiting for server response. It will cover the global timeout set for the server by using the command "tacacs timeout"
integer2	(optional) Setting the value of timeout timer. It is calculated on second.
key	(optional) Designating authentication and encryption key. The

	secret key shall match with the one used by the program of TACACS+ server. Designating this. It will cover all keys set for the server by command "tacacs key".
string	(optional) Specifying the encrypted key.

Default Value

Disabled

Command Mode

Global configuration mode

Usage Guidelines

The command can be used to search a host according to the specified order by command tacacs-server plus host. As some parameters of tacacs-server host will cover all configurations of commands "tacacs-server timeout" and "tacacs-server key"in global mode, the command can set the communication attribute of each TACACS+ server exclusively. Thus, the security of the network enhanced.

Example

The following example shows how the designated server negotiates with TACACS+ server whose IP address is 1.1.1.1 and carries out AAA authentication. The command can also designate the TCP port number of the server to 51, the timeout is 3 seconds and the encryption key is tacacs-server key.

tacacs -server host 1.1.1.1 single-connection port 51 timeout 3 key a_secret

3.1.4 tacacs-server key

Syntax

To set the encryption key of the communication process between the device and TACACS+ server, run command tacacs-server key in global mode. To return to the default setting, use the no form of this command.

tacacs-server key
no tacacs-server key

Parameters

Parameters	Description
key	Uses for setting encryption key. The secret key shall match with the one used by the program of TACACS+ server.

Command Mode

Global configuration mode

Usage Guidelines

You must set the encryption key by command tacacs-server key before running TACACS+ protocol. The key must correspond to the key used by TACACS+ server program. All sentence-initial spaces will be ignored and there cannot be any space in the middle of the key.

Example

The following example shows how to set the encryption key as testkey.
tacacs-server key testkey

3.1.5 tacacs-server timeout

Syntax

To set the timeout of TACACS+ waiting for a server reply, run command tacacs-server timeout in global configuration mode. To return to the default setting, use the no form of this command.
tacacs-server timeout *seconds*
no tacacs-server timeout

Parameters

Parameters	Description
seconds	The timeout in seconds (ranges from 1 to 600) The default value is 5 seconds.

Default Value

5 seconds

Command Mode

Global configuration mode

Usage Guidelines

If the command tacacs-server sets timeout, it will cover the global timeout set by the command before.

Example

The following example shows how to change the timeout to 10 seconds:
tacacs-server timeout 10