Security Configuration Commands

As our products undergo continuous development the specifications are subject to change without prior notice.

Table of Contents

Chapter 1 AAA Configuration Commands

This chapter describes the commands used to configure AAA authentication methods. Authentication identifies users before they are allowed access to the network and network services.

1.1 AAA Authentication Configuration Commands

For information on how to configure authentication using AAA methods, refer to the "Configuring Authentication" chapter. For configuration examples using the commands in this chapter, refer to the "Authentication Examples" section located at the end of the "Configuring Authentication" chapter.

AAA 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 the login banner, run the following command. To return to the default setting, use the no form of this command.

aaa authentication banner delimiter string delimiter

no aaa authentication banner

Parameter

Parameter	Description

delimiter string delimiter	String shown when the user logs in. The delimiter is “”.

Default

The default banner is:

User Access Verification

Command Mode

Global configuration mode

Usage Guidelines

To create a banner, you have to configure a delimiter and then the text character string. The delimiter is to notify the system that its following text character string will be shown as the banner. The delimiter appears repeatedly at the end of the text character string, indicating that the banner is end.

Example

The following example shows how to change the login banner to the following character string:

aaa authentication banner “Welcome to XXCOM system!”

Related Command

aaa authentication fail-message

1.1.2 aaa authentication fail-message

Syntax

To configure the failed-login banner, run the following command. To return to the default setting, use the no form of this command.

aaa authentication fail-message delimiter string delimiter

no aaa authentication fail-message

Parameter

Parameter	Description
delimiter string delimiter	String shown when the user logs in. The delimiter is “”.

Default

The default failed login banner:

Authentication failed!

Command Mode

Global configuration mode

Usage Guidelines

To create a banner, you have to configure a delimiter and then the text character string. The delimiter is to notify the system that its following text character string will be shown as the banner. The delimiter appears repeatedly at the end of the text character string, indicating that the banner is end.

Example

The following example shows how to change the failed-login banner 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 username prompt, run the following command. To return to the default setting, use the no form of this command.

aaa authentication username-prompt text-string

no aaa authentication username-prompt

Parameter

Parameter	Description
text-string	Text shown when the username prompt appears.

Default

The username prompt character string is “Username” when there is no defined text string.

Command Mode

Global configuration mode

Usage Guidelines

The command “aaa authentication username-prompt” can be used to change the character string of the username prompt.

Username:

Some protocols (such as TACACS+) are capable of overlapping the local user name prompt information. In this circumstance, command “aaa authentication username-prompt” doesn’t change the character string of the user name prompt.

Note:

The command **aaa authentication username-prompt** doesn’t change any prompt information provided by remote TACACS+ or RADIUS server.

Example

The following example shows how to change the character string of the username prompt to the following character string:

aaa authentication username-prompt “YourUsernam:”

Related Command

aaa authentication password-prompt

1.1.4 aaa authentication password-prompt

Syntax

To change the text displayed when users are prompted for a password, use the aaa authentication password-prompt global configuration command. Use the no form of this command to return to the default password prompt text.

aaa authentication password-prompt text-string

no aaa authentication password-prompt

Parameter

Parameter	Description
test-string	String of text that will be displayed when the user is prompted to enter a password.

Default

There is no user-defined text-string, and the password prompt appears as "Password:"

Command Mode

Global configuration mode

Usage Guidelines

Use the **aaa authentication password-prompt** command to change the default text that the software displays when prompting a user to enter a password. This command changes the password prompt for the enable password as well as for login passwords that are not supplied by remote security servers. The no form of this command returns the password prompt to the default value:

Password:

The **aaa authentication password-prompt** command does not change any dialog that is supplied by a remote TACACS+ server or RADIUS server.

Example

The following example shows how to change the text of the username prompt to “Your Password:”

aaa authentication password-prompt “YourPassword:”

Related Command

aaa authentication username-prompt

enable password

1.1.5 aaa authentication dot1x

Syntax

To configure dot1x access authentication, run the following command. To return to the default setting, use the no form of the above command.

aaa authentication dot1x {**default** | *list-name*} *method1* [*method2...*]

no aaa authentication dot1x {**default** | *list-name*}

Parameter

Parameter	Description
Default	Use the authentication method following the Parameteras the default method
list-name	The character string used to name the authentication method list. The method in the authentication method list will be activated when the user accesses the authentication.
method	At one keyword described by “dot1x authentication method”.

Default

The authentication return will be failed if the authentication method is not configured.

Command Mode

Global configuration mode

Usage Guidelines

The default list or other defined lists created by the command **aaa authentication dot1x** will be quoted by dot1x application and thus the dot1x user will be authenticated.

The next authentication method will be adopted only when the former method is failed. Other authentication method will not be adopted if the former authentication method return is failed.

dot1x Authentication Method

Keyword	Description
group name	Uses the server group for authentication
group radius	Uses tacacs for authentication
group tacacs+	Uses TACACS+ for authentication

local	Uses the local user name data base for authentication
local-case	Uses case-sensitive local username for authentication.
none	Uses no authentication.

Example

The following example shows how to create an authentication method list named “TEST”. The authentication first tries to connect with TACACS+ server. If no result (either “success” or “failure”) is acquired from the TACACS+ server group (no dead error returned from TACACS+ server), try another method: local. If the local method can’t acquire accurate result either, the internet can be accessed without authentication. (Up to now the device’s authentication methods including aaa system enable(line) and local can acquire an accurate result either success or failure. Therefore, the following command has no none method.)

aaa authentication dot1x TEST group tacacs+ local none

The following example shows how to create a same list but configured with default list. If no other list is designated, the list is available to all dot1x authentications.

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. Use the no form of this command to disable this authentication method.

aaa authentication enable default method1 [method2...]

no aaa authentication enable default

Parameter

Parameter	Description
method	At least one of the keywords described in “enable authentication method”.

Default

The authentication method is not configured. The authentication process returns successfully if the user is the console port. Otherwise, the authentication process fails.

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.

Table 0-1 aaa authentication enable default Methods

Keyword	Description
enable	Uses the enable password for authentication.
group name	Uses the server group for authentication.
group radius	Uses RADIUS for authentication.
group tacacs+	Uses tacacs+ for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.

Example

The following example shows how to create an authentication method list named “TEST”. The authentication first tries to connect with TACACS+ server. If no result (either “success” or “failure”) is acquired from the TACACS+ server group (no dead error returned from TACACS+ server), try another method: local. If the local method can’t acquire accurate result either, the internet can be accessed without authentication. (Up to now the device’s authentication methods including aaa system enable(line) and local can acquire an accurate result either success or failure. Therefore, the following command has no 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}

Parameter

Parameter	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 “login authentication method”.

Default

The authentication method is not configured. The authentication process returns successfully if the user is the console port. Otherwise, the authentication process fails.

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.

If authentication is not specifically set for a line, the default is to deny access and no authentication is performed.

AAA authentication login Methods

Keyword	Description
enable	Uses the enable password for authentication.
group name	Uses the server group for authentication.
group radius	Uses RADIUS for authentication.
group tacacs+	Uses tacacs+ for authentication
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
localgroup	Uses the local strategy group user name database for

	authentication.
local-case	Uses case-sensitive local username for 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, enter the aaa group server radius command in global configuration mode. To remove a group server from the configuration list, enter the no form of this command.

aaa group server {radius | tacacs+} group-name

no aaa group server {radius | tacacs+} group-name

Parameter

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

Default

No server group.

Command Mode

Global configuration mode

Usage Guidelines

The authentication, authorization, and accounting (AAA) server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service. It can set 63

server groups at most.

Example

The following example adds a radius server group named radius-group:

aaa group server radius radius-group

Related Command

server

1.1.9 server

Syntax

To add a server in the AAA server group, use the server command in server-group configuration mode. To remove the associated server from the authentication, authorization, and accounting (AAA) group server, use the no form of this command.

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 in the radius server group, use the following command:

server {A.B.C.D | X:X:X:X::X} [**key** {*password* | {*encryption-type encrypted-password*}}]

no server A.B.C.D

Parameter

Parameter	Description
A.B.C.D	IP address of the server.
X:X:X:X::X	IPv6 address of the server
key	key
password	the character string of the key
encryption-type	Encryption type, 0 means no encryption, 7 means encryption
encrypted-password	Encryption password character string corresponding to the encryption type
auth-port	authentication destination port
acct-port	account port

num	port number
retransmit value	Retransmit times, the default is twice
timeout value	Timeout for retransmit; the default is 3 seconds.
privilege pri	Server priority; the default is 0.

Default

No server

Command Mode

Server-group configuration

Usage Guidelines

You can set 63 server groups in maximum, 1 radius server chain table and 1 tacacs+ server chain table. The total of all radius server groups and server groups in the server chain tables is 64. The total of all tacacs+ server groups and server groups in the server chain tables is also 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 display information on authentication, authorization, and accounting (AAA) TACACS+ authentication, use the **debug aaa authentication** command in privileged EXEC mode. To disable debugging output, use the no form of this command.

debug aaa authentication

no debug aaa authentication

Parameter

None

Default

Disable debug information

Command Mode

EXEC mode

Usage Guidelines

Use this command to learn the methods of authentication being used and the results of these methods.

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 in global configuration mode. 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*]

Parameter

Parameter	Description
password	Password users type to enter enable mode.
encryption-type	Algorithm used to encrypt the password.
encrypted-password	Encrypted password you enter, copied from another router configuration.
level	Level for which the password applies.
number	Number between 1 and 15 that specifies the privilege level for the user.

Default

No password is defined.

Command Mode

Global configuration mode

Usage Guidelines

There cannot have spaces in the password that the router configures. When using the enable password command, you cannot input space if you enter a clear text password. The length of the clear text password cannot exceed 127 characters.

The default level Parameter is 15 without inputting the level Parameter. If a privilege level is not configured password, then no authentication is performed when a user entering this privilege level.

Our system only supports two types of encryption. The encryption type is 0 and 7 respectively. Parameter 0 indicates no password is defined and you enter a clear text password in the following encrypted-password blank. Parameter 7 indicates a self-defined algorithm is used for encryption and you enter encrypted text password in the following encrypted-password blank. This encrypted text password can be copied from the configuration file of other device.

Example

The following example adds password clever for the privilege level 10, uses encryption-type 0, that is, the clear text password:

enable password 0 clever level 10

The following example adds password Oscar for the default privilege (15), uses encryption-type 7, that is, the encrypted text password:

enable password 7 074A05190326

Assuming the encrypted text password of Oscar is 074A05190326, which is obtained from the configuration file of other router.

Related Command

aaa authentication enable default

service password-encryption

1.1.12 enable(enter)

Syntax

To enter the EXEC mode when logging in the system, run **enable(enter)** command.

enable(enter) <1-15>

Parameter

Parameter	Description
<1-15>	To be obtained privilege priority

Default

Do not enter the privileged mode.

Command Mode

User mode

Usage Guidelines

None

Example

>enable(The user is 15 by default.)

Password: (To authenticate by entering the password)

#

#exi

>enable 1(To be obtained privilege priority is 1.)

Password:(Enter 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 in global configuration mode. To restore the default, use the no form of this command.

service password-encryption

no service password-encryption

Parameter

None

Default

No encryption

Command Mode

Global configuration mode

Usage Guidelines

Currently in the realization of our router system, this command is related to username password, enable password and password. If this command is not configured on the router (namely default state), and the system uses the clear text storage method in the above three commands, then the configured clear text of the password can be displayed in the show running-config command. If this command is configured on the router, then the configured password of the above three commands will be encrypted, then the configured clear text of the password cannot be displayed in the show running-config command, even using the no service password-encryption cannot restore the clear text of the password. Please make sure of the configured password before using this command for encryption. The no service password-encryption command only has effect on the password configured by the service password-encryption command.

Example

Use the following command to encrypt for the configured clear text password and also to encrypt for the clear text password that configured after using this command.

switch_config#service password-encryption

Related Command

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

1.2 AAA Authorization Configuration command

This section 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.

The authorization 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. The “no” format of the command can be used for closing the authorization of some function.

aaa authorization {{commands <*0-15*>**} | network** | **exec}** {**default** | *list-name*} *method1* [*method2...*]

no aaa authorization {{commands <*0-15*>**} | network** | **exec}** {**default** | *list-name*}

aaa authorization config-commands

no aaa authorization config-commands

Parameter

Parameter	Description
commands	EXEC (shell) command authorization
<*0-15*>	Priority of the to be authorized command
network	The authorization of network type service, such as PPP, SLIP.
exec	It is applicable to the attribute related to the user EXEC terminal dialogue. It determines whether the EXEC shell program can be enabled when users register the system or authorize users the priority of entering EXEC shell.
default	Default authorization methods list
list-name	The character string used for naming authentication methods list.
method	One of the keywords listed in the form below.
config-commands	Configuration mode command service

Default

When the user requests for authorization and the authorization methods list required for use is not designated on the corresponding line or the interface, the default authorization methods list will be used. If default methods list is defined, no authorization will take place.

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 methods list defines the method for authorization implementation and sequence for executing these authorization methods. The methods list is only a simple naming list describing the authorization method for inquiry on the sequence (such as RADIUS and TACACS+). The methods list can designate one or multiple security protocols used for authorization. So it is able to guarantee a backup method in case all the above listed 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.

Keyword of AAA Authorization:

Keyword	Description
group name	Uses group name for authorization.
group radius	Uses radius for authorization.
group tacacs+	Uses tacacs+ for authorization.
if-authenticated	Uses if-authenticated for authorization.
local	Uses the local database for authorization.
none	Uses no authentication.

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 PPP. 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 authorization process, use debug **aaa authorization** command. To return to the default setting, use the no form of this command.

debug aaa authorization

no debug aaa authorization

Parameter

None

Default

Disable debug information.

Command Mode

EXEC mode

Usage Guidelines

The command is used to track the authorization process of each user, so that the reason of failure can be found.

Example

None

Related command

None

1.3 Accounting Command

This section describes the commands for configuring AAA authentication methods. 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 router will report user's activities to the TACACS+ server or the RADIUS server in the accounting record 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.

Authentication 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*}

Parameter

Parameter	Description
commands	EXEC (shell) command authorization
<0-15>	Priority of the to be authorized command
network	The authorization of network type service, such as PPP, SLIP.
exec	It is applicable to the attribute related to the user EXEC terminal dialogue.
connection	Provides information about all egress connections from related router. Currently, only the H323 session is supported.
default	Default authorization methods list
list-name	The character string used for naming authentication methods list.
Start-stop	Start and stop accounting
Stop-only	Stop accounting
None	No accounting
group *groupname*	Uses the server group for accounting
group radius	Uses RADIUS for accounting
group tacacs+	Uses TACACS+ for accounting

Default

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**}

Parameter

Parameter	Description
update	Activates the router to transmit temporary accounting records.
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

Temporary accounting activity does not occur.

Command Mode

Global configuration mode

Usage Guidelines

The function works with the support of the application end. Therefore, it is inapplicable 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. You can run no aaa accounting suppress null-username to resume the default configuration.

aaa accounting suppress null-username

no aaa accounting suppress null-username

Parameter

None

Default

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 accounting process, use debug aaa accounting command. To return to the default setting, use the no form of this command.

debug aaa accounting

no debug aaa accounting

Parameter

None

Default

Disable debug information.

Command Mode

EXEC mode

Usage Guidelines

The command is used to track the accounting process of each user, so that the reason of failure can be found.

Example

None

Related Command

None

1.4 Local Account Policy Configuration Commands

The section describes the commands for local account policy configuration. The local account policy is used for local authentication and local authorization.

For information on how to configure local account policies, see “configuring local account policies”. If you want to see an example of configuring using the commands in this section, read the example section at the end of the "configuring local account policy" document.

The 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 the local authentication policy, run **localauthen** command in the global configuration mode. To return to the default setting, use the no form of this command.

localauthen *WORD*

no localauthen *WORD*

Parameter

Parameter	Parameter Description
WORD	name of local authentication policy

Default

None

Command Mode

Global Configuration Mode

Usage Guidelines

Enter the local authentication policy configuration, use localauthen WORD command. Use the following command to configure the local authentication policy:

- The maximum tries with a certain time:

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

Parameter	Parameter Description
max-tries	the maximum tries
<1-9>	The maximum tries ranges from 1 to 9.
try-duration	The duration for login trial.
1d2h3m4s	The format of day, hour, minute and second.

Related Command

login max-tries

localgroup

local authen-group

username

1.4.2 localauthor

Syntax

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

localauthor *WORD*

no localauthor *WORD*

Parameter

Parameter	Parameter Description
WORD	Name of the local authorization policy

Default

None

Command Mode

Global Configuration Mode

Usage Guidelines

Enter the local authorization policy configuration, use **localauthen WORD** command. Use the following command to configure the local authorization policy:

To authorize the priority for the login user

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

Parameter	Parameter Description
default	The default priority (when the concrete login method is not configured, authorize by the priority.)
console	The authorization priority of the login user in the console port.
ssh	The authorization priority of the ssh login user
telnet	The authorization priority of the telnet login user
<*1-15*>	Priority

Related Command

exec privilege

localgroup

local author-group

username

1.4.3 localpass

Syntax

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

localpass *WORD*

no localpass *WORD*

Parameter

Parameter	Parameter Description
WORD	Name of local password policy

Default

None

Command Mode

Global Configuration Mode

Usage Guidelines

Enter the localpass WORD policy configuration, use localpass WORD command. Use the following command to configure the local password policy:

- The password and username is different

  non-user

- History password check (It is different with the history password when modifying the user password)

  non-history

- Designate the password content

  element *[number] [lower-letter] [upper-letter] [special-character]*

Parameter	Parameter Description
number	It must include numbers.
lower-letter	It must include the lower letter.
upper-letter	It must include the upper letter.
special-character	It must include the special character.

- The minimum length of the password:

  min-length *<1-127>*

Parameter	Parameter Description
<1-127>	The minimum length (The range is 1-127)

- The password validity:

  validity *1d2h3m4s*

Parameter	Parameter Description
1d2h3m4s	The format of day, hour, minute and second.

Related Command

non-use

non-history

element

min-length

validity

localgroup

local pass-group

username

1.4.4 localgroup

Syntax

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

localgroup *WORD*

no localgroup *WORD*

Parameter

Parameter	Parameter Description
WORD	Name of the local policy group

Default

None

Command Mode

Global Configuration Mode

Usage Guidelines

Enter the localgroup WORD policy configuration, use localpass WORD command. Use the following command to configure the local password policy:

- **local authen-group**
- **local author-group**

- **local pass-group**
- **local user**
- **username**

Related Commands

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 the local authentication group, run local authen-group command. The local authentication group is by default in the global configuration mode. To return to the default setting, use the no form of this command.

local authen-group *WORD*

no local authen-group

Parameter

Parameter	Parameter Description
WORD	Name of local authentication group

Default

None

Command Mode

Global configuration mode, local policy group configuration mode

Usage Guidelines

None

Related commands

localauthen

localgroup

local authen-group

1.4.6 local author-group

Syntax

To configure the local authorization group, use the local author-group command. The local authorization group is by default in the global configuration mode. To return to the default setting, use the no form of this command.

local author-group *WORD*

no local author-group

Parameter

Parameter	Parameter Description
WORD	Name of the local authorization group

Default

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

local pass-group *WORD*

no local pass-group

Parameter

Parameter	Parameter Description

WORD	Name of the local password group

Default

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 connections and freeze users of the account configured in the local group, run **local user** command. The local user group is by default in the 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* }**}**

Parameter

Parameter	Parameter Description
maxlinks	Limit the number of login users simultaneously for one user name
<1-255>	amount (range from 1-255)
freeze	freeze users
WORD	user name

Default

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 the following command. The username is by default in the 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*

Parameter

Parameter	Parameter Description
username	user name character string
password	username 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	Links established by the account (the number of simultaneous login users of one user name)
number	the number of links
authen-group	Designate local authen-group
WORD	Name of local authen-group
author-group	Designate local author-group

WORD	Name of local author-group
pass-group	Designate local pass-group
WORD	Name of local pass-group
autocommand	Auto run the designated command after the user logs in. The auto command must be used at the end of the command line.
command	Auto run the command character string.
Non-supported options	
bind-ip	binding IP address (non-supported)
A.B.C.D	IP address
bind-mac	Binding user mac address (non-supported)
H:H:H:H:H:H	ARP recorded 48 byte hardware address
bind-pool	Binding user address pool (non-supported)
WORD	Address pool name
bind-port	Binding user port (non-supported)
port	Port
callback-dialstring	Call back telephone number (non-supported)
string	Telephone number character string;
callback-line	The line used in call back (non-supported)
line	ine number
callback-rotary	Call back rotary configuration (non-supported)
rotary	Rotary number
nocallback-verify:	No callback verification (non-supported)
nohangup	No hangup after the user logs in and auto run the command (non-supported)

noescape	No escape character after the user logs in (non-supported)

Default

None

Command Mode

Global configuration mode, local policy group configuration mode

Usage Guidelines

The password is empty character string when there is no password parameter.

User-maxlinks limit the established number of sessions simultaneously in one account. The session will not be count in if it is not authenticated by the local auth-group. To check the basic information of teach online user, run show aaa users command.

Our system only supports two types of encryption. The encryption type is 0 and 7 respectively. Parameter 0 indicates no password is defined and you enter a clear text password in the following encrypted-password blank. Parameter 7 indicates a self-defined algorithm is used for encryption and you enter encrypted text password in the following encrypted-password blank. This encrypted text password can be copied from the configuration file of other device.

Example

The following example shows how to add local users whose user name is someone and whose password is someother:

username someone password someother

The following example shows how to add the local user whose name is Oscar and whose password is Joan. The adopted encryption-type is 7. Enter the password ciphertext:

enable password 7 1105718265

Suppose that the cipher text of Joan is 1105718265, the value of the cipher text is obtained from the configuration files of other routers.

Related command

aaa authentication login

1.4.10 show local-users

Syntax

To show the overview of all local AAA account, run show local-users command.

show local-users

Parameter

None

Default

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to show all AAA accounts which include 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:	local group
links	Links used by the account (It is how many users are using.)
pw_present	Password presence time (configure the valid password period)
login_tries	Password matching failure times (set the max login tries, 0 means no setting.)
login_try_time	Timeout of password matching failure (se the max login tries, 0 means no setting.)
freezing_cause	Reason of account freezing.

Related command

username

1.4.11 show aaa users

Syntax

To show the overview of all online AAA users, run show aaa users command.

show aaa users

Parameter

None

Default

None

Command Mode

EXEC mode

Usage Guidelines

The command can be used to show information of all online users such as port, username, service type (service), online duration (time) and IP address (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 describes the commands used to configure RADIUS. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the implementation, RADIUS clients run on routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

For information on how to configure RADIUS, refer to the chapter "Configuring RADIUS".

2.1 RADIUS Configuration Commands

RADIUS Configuration Commands include:

- debug radius
- ip radius source-interface
- radius-server acct-on
- 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 display information associated with RADIUS, use the debug radius command in EXEC mode. To disable debugging output, use the no form of this command.

debug radius {*event* | *packet*}

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

Parameter

Parameter	Description
event	Displays radius event
packet	Displays radius packet.

Default

None

Command Mode

EXEC mode

Usage Guidelines

The command can be used to debug network system to locate the authentication failure reason.

Example

The following example debugs RADIUS event:

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

Parameter

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

Default

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 router has many subinterfaces and you want to ensure that all RADIUS packets from a particular router 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 transmit some attributes in radius AAA, run the following command. To return to the default setting, use the no form of this command.

radius-server attribute {**4** | **32 | 95**}

no radius-server attribute {**4** | **32 | 95**}

Parameter

Parameter	Parameter Description
4	Transmit the value of attribute 4 (NAS ip address) after the parameter in dealing with the radius.
32	Designate the transmission attribute 32 (NAS identifier) in radius authentication and accounting according to the command after the parameter.
95	Designate the transmission attribute 95 (NAS ipv6 address) in radius authentication and accounting according to the command after the parameter.

Default

None

Command Mode

Global configuration mode

Usage Guidelines

Use radius-server attribute command to designate a certain attribute in dealing with radius.

Use radius-server attribute 4 (NAS IP address) and designate transmission in RADIUS packet.

Designate the transmission attribute 32 (NAS identifier) in radius authentication and accounting according to the command after the parameter.

Designate the transmission attribute 95 (NAS ipv6 address) in radius authentication and accounting according to the command after the parameter.

Example

radius-server attribute 4 X.X.X.X transmits radius attribute 4 in RADIUS packet and use X.X.X.X as the attribute value

radius-server attribute 32 in-access-req transmits NAS identifier in authentication request

radius-server attribute 32 in-account-req transmits NAS identifier in accounting request

radius-server attribute 32 identifier configures NAS identifier

radius-server attribute 95 X:X:X:X::X transmits radius attribute 95 in RADIUS packet and use X:X:X:X::X as the attribute value

Related Command

None

2.1.4 radius-server challenge-noecho

Syntax

To prevent user responses to Access-Challenge packets from being displayed on the screen, use the radius-server challenge-noecho command in global configuration mode. To return to the default condition, use the no form of this command.

radius-server challenge-noecho

no radius-server challenge-noecho

Parameter

None

Default

All user responses to Access-Challenge packets are echoed to the screen.

Command Mode

Global configuration mode

Usage Guidelines

None

Example

radius-server challenge-noecho

2.1.5 radius-server deadtime

Syntax

To improve RADIUS response times when some servers might be unavailable and cause the unavailable servers to be skipped immediately, use the radius-server deadtime command in global configuration mode. To set dead-time to 0, use the no form of this command.

radius-server deadtime minutes

no radius-server deadtime

Parameter

Parameter	Description
minutes	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours).

Default

Dead time is set to 0.

Command Mode

Global configuration mode

Usage Guidelines

Use this command to cause the software to mark as "dead" any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before trying the next configured server. A RADIUS server marked as "dead" is skipped by additional requests for the duration of minutes or unless there are no servers not marked "dead."

Example

The following example specifies five minutes deadtime for RADIUS servers that fail to respond to authentication requests:

radius-server deadtime 5

Related Command

radius-server host

radius-server retransmit

radius-server timeout

2.1.6 radius-server directed-resquest

Syntax

To designate RADIUS server with the format of '@server', run radius-server directed-resquest command in the global configuration 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]

Parameter

Parameter	Parameter description

restricted	Only enable the user to designate RADIUS server with the format of '@server'

Default

It doesn’t support to designate RADIUS server with the format of '@server'.

Command Mode

Global configuration mode

Usage Guidelines

None

Example

radius-server directed-resquest

Related Command

None

2.1.7 radius-server host

Syntax

To specify a RADIUS server host, use the radius-server host command in global configuration mode. To delete the specified RADIUS host, use the no form of this command.

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

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

Parameter

Parameter	Description
ip-address	IP address of the RADIUS server host.
ipv6-address	IPv6 address of the RADIUS server host.
auth-port	(Optional) Specifies the UDP destination port for authentication requests.
port-number1	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0.
acct-port	(Optional) Specifies the UDP destination port for accounting requests.
port-number2	(Optional) Specifies the UDP destination port for accounting requests; the host is not used for accounting if set to 0.

Default

No RADIUS host is specified;

Command Mode

Global configuration mode

Usage Guidelines

You can use multiple radius-server host commands to specify multiple hosts. The software searches for hosts in the order in which you specify them.

Example

The following example specifies host 1.1.1.1 as the RADIUS server and uses default ports for both accounting and authentication

radius-server host 1.1.1.1

The following example specifies port 12 as the destination port for authentication requests and port 16 as the destination port for accounting requests on the RADIUS host named host1:

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

To set the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon, use the radius-server key command in global configuration mode. To disable the key, use the no form of this command.

radius-server key *string* | {encryption-type encrypted-password}

no radius-server key

Parameter

Parameter	Description
string	Spedifies the encrypted key. This encrypted key must match the encrypted key that RADIUS server uses.

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

The encrypted key is the empty character string.

Command Mode

Global configuration mode

Usage Guidelines

The key entered must match the key used on the RADIUS daemon. All leading spaces are ignored, and all white spaces cannot be included in the encrypted key.

Example

The following example sets the encryption key to " firstime ":

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 restore the default, use the no form of this command.

radius-server optional-passwords

no radius-server optional-passwords

Parameter

This command has no Parameters or keywords.

Default

Disabled

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

Parameter

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

Default

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 restore the default, use the no form of this command.

radius-server timeout *seconds*

no radius-server timeout

Parameter

Parameter	Description
seconds	Number that specifies the timeout interval, in seconds. The default is 3 seconds.

Default

3 seconds

Command Mode

Global configuration mode

Usage Guidelines

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

Example

Use this command 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 radius-server vsa send command. To restore the default, use the no form of this command.

radius-server vsa send [**authentication**]

no radius-server vsa send [**authentication**]

Parameter

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

Default

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 accounting keyword with the radius-server vsa send command to limit the set of recognized vendor-specific attributes to just accounting 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

2.1.13 radius-server acct-on

Relevant configuration about accounting function.

[no] radius-server acct-on enable

Open/close radius accounting function.

[no] radius-server acct-on retransmit <1-15>

Set the time of radius accounting retransmit, the default is 3times.

Parameter

Parameter	Description
Retransmit	Times of radius accounting retransmit

Default

Close accounting function, the retransmit is 3 times.

Command mode

Global configuration mode

Usage Guidelines

None

Example

The following example configures the switch. Open the accounting function, set the retransmit times as 5:

radius-server acct-on enable

radius-server acct-on retransmit 5

Related Command

None

Chapter 3 TACACS+ 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.

For information and examples of how to configure TACACS+, see “configuring TACACS+”.

3.1 TACACS+ 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

The command “debug tacacs” can be used for tracing TACACS+protocol event or checking the packets received or sent. The “no” format of the command can be used for canceling the trace.

debug tacacs {**event** | **packet**}

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

Parameter

Parameter	Description
event	***Tracing*** *TACACS+ event*
packet	**Tracing** TACACS+ packet.

Default

Disable debug information

Command Mode

EXEC mode

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 will open the event trace of TACACS+

debug tacacs event

Related Command

None

3.1.2 ip tacacs source-interface

Syntax

The global configuration command “ip tacacs source-interface” is used for applying IPaddress of the designated interface to all the TACACS+ packets. The “no” format of the command cancel the using of the IP address.

ip tacacs source-interface *subinterface-name*

no ip tacacs source-interface

Parameter

Parameter	Description
subinterface-name	Interface name corresponding to the source IP address of all TACACS+

Default

None

Command Mode

Global configuration mode

Usage Guidelines

The command can be used to set source IP address for all TACACSpackets 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 s1/0 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

The command “tacacs-server host” can be used for designating TACACS+ server, run tacacs-server host command. To return to the default setting, use the no form of this command.

tacacs-server host *ip-address* [**single-connect**|**multi-connect**] [**port** *integer1*] [**timeout** *integer2*] [**key** *string*]

no tacacs-serve *ip-address*

Parameter

Parameter	Parameter Description
ip-address	IP address of the server
single-connect	(optional) Maintain a single open TCP connection from AAA/TACACS+ server.
multi-connect	(optional) Maintain multiple TCP connections from AAA/TACACS+ server.
port	(optional) Set port number. The option covers up the default port number 49.
integer1	(optional) The port number of the server. The effective port number ranges from 1 to 65536.
timeout	(optional) Set timeout value of the server. It covers up the global timeout value for the server by tacacs command.
integer2	(optional) Set timeout value by seconds.
key	(optional) Set authentication and encryption key. The key must be match with the key of TACACS+ server program. The key covers up the server key of global tacacs key.
string	(optional) Set encryption key character string.

Default

No TACACS+ server is set.

Command Mode

Global Configuration Mode

Usage Guidelines

Use tacacs-server commands to set multiple hosts and explore the host in order. As some parameters of tacacs-server host command cover up configurations tacacs-server timeout and tacacs-server key commands set in global configuration mode. Therefore, the command can configure the communication attribute of each TACACS+ server.

Example

The following example shows how to negotiate the router and TACACS+ server whose IP address is 1.1.1.1 (for AAA) and set the TCP service port of the server as 51. The timeout value is 3 seconds and the encryption key is a_secret.

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 keys between the router and TACACS+ server, run tacacs-server key command in the global configuration mode. To return to the default setting, use the no form of this command.

tacacs-server key

no tacacs-server key

Parameter

Parameter	Parameter Description
key	It is used for setting the encryption key. The encryption key must be match with the key of TACACS+ server program.

Command Mode

Global Configuration Mode

Usage Guidelines

The encryption key must be set by tacacs-server key command before running TACACS+ protocol. The encryption key must be match with the key of TACACS+ service program. All spaces must be avoided.

Example

The following example shows how to set the encryption key as testkey:

tacacs-server key testkey

3.1.5 tacacs-server timeout

Syntax

The command “tacacs timeout” can be used to set the length of timeout for TACACS+ to wait for the response from some server. The “no” format of the command can be used for restoring default value.

tacacs timeout *seconds*

no tacacs timeout

Parameter

Parameter	Description
seconds	The value of timeout calculated on second (between 1 to 600). The default value is 5 seconds.

Default

5 seconds

Command Mode

Global configuration mode

Usage Guidelines

If some server sets its own timeout value of waiting through the parameter in the command “tacacs server”, the value will cover the global timeout value set by this command.

Example

The Example below changes the value of timeout timer as 10 seconds.

```
tacacs-server timeout 10
```