Security Configuration Commands

Table of Contents

Chapter 1 **AAA Configuration Commands**

1.1 Authentication Commands

This Chapter describes the commands used for configuring the AAA authentication method. Authentication defines the access right of the users before they are allowed to access the network and network services.

Please refer to “Configuration 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.

1.1.1 aaa authentication enable default

AAA authentication shall be enabled so as to determine whether a user has the access to the command of privileged priority by using the command “aaa authentication enable default”. The authentication method can be closed by using the “no” format of the said command.

Syntas

aaa authentication enable default *method1* [*method2...*]

no aaa authentication enable default *method1* [*method2...*]

Parameter

The **method** parameter is one of the key words at least in list 1.

Default

If default is not set, the enable password shall be used to make authentication, it has the same effect as the command below.

aaa authentication enable default enable

If the enable password exists in configuration list, the password should be used. If no password is set, the final feedback result will recognize the success of authentication.

Command mode

global configuration mode

Explanation

The command “aaa authentication enable default” can be used to create a series of authentication methods, which are used to determine whether a user has the right to use the privileged commands. The keyword “method” has been explained in form 1. Only when the previous authentication method feeds back error, other authentication methods shall be applied. If the feedback result of the said authentication method informs the failure of the authentication, other authentication method shall be employed. If all the authentication method is expected to feed back the result of failure and the authentication still succeeds, “none” can be designated as the last authentication method of command line.

On top of that, when the method of RADIUS or TACACS+ is available for making authentication of enable, the user names applied are different. The user name shall be “$ENABLE*level*$” in case “RADIUS” is used for authentication. The “level” in the user name refers to the privileged level accessible to the user. When TACACS+ is used for authentication, the user name is the one used when the user log on the router. The relevant specific configuration can be referred to as the part of “AAA Authentication Configuration” in the document.

Figuer 1-1 Effective Default Method of AAA Authentication

Keyword	Description
group	The server group is used for authentication
group-restrict	The server group is used for authentication. But when the user designates a server, the server group is disabled.
enable	The enable password is used for authentication.
line	The password line is used for authentication
none	Authenticating the passage of none condition
tacacs+	TACACS+ is used for authentication
radius	RADIUS is used for authentication.

Example

An authentication list is created in the following example. The list first tries to connect with TACACS+ server. If no error is fed back by TACACS+ server or no server is found, AAA will try using the enable password. Should the error be fed back to such trial (as no effective password is configured on the server), the user will be allowed to access the server without authentication.

aaa authentication enable default tacacs+ enable none

Related command

enable password

1.1.2 aaa authentication login

The global configuration command “aaa authentication login” shall be used for setting AAA authentication at the time of login. The “no” format of the command can be used to close AAA authentication.

Syntas

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

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

Parameter

Parameter	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 is used to name the character string of authentication method list. When the user logs in, the methods listed in authentication method list will be activated.
method	It is one of the key words described in the Form 2 at the least.

Default

If no default method list is set, the default will not make authentication. At this moment, it has the same effect as the one below:

aaa authentication login default none

Command mode

global configuration mode

Explanation

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 feed back the failure, no other authentication methods will be used. To ensure the success of authentication even if all authentication methods feed back error, “none” shall be designated as the last method of the command line.

If no authentication is specially set for a line, no authentication will be executed at the time of default.

Figuer 1-2 The Registration Method of AAA Authentication

Key Word	Description
enable	The enable password is used for authentication
group	The server group is used for authentication
group-restrict	The server group is used for authentication. But when the user designates a server, the server group is disabled.
line	The password line is used for authentication
local	The database of local user names is used for authentication.
local-case	The database of local user names is used for authentication (case sensitive for user name)
none	No authentication is made.
radius	RADIUS is used for authentication
tacacs+	TACACS+ is used for authentication.

Example

AAA authentication methods list named “TEST” is created in the following example. This authentication first tries to connect with TACACS+ server. If no error is fed back by TACACS+ or no server is found, AAA will try using the enable password. Should error be fed back to such attempt (as no enable password is configured on the router), the user will be allowed to access the network without authentication.

aaa authentication login TEST tacacs+ enable none

The same list is created in the Example below, but the default list is set. If no other lists are designated, the list will be used for all the login authentication.

aaa authentication login default tacacs+ enable none

Relevant command

None

1.1.3 aaa authentication ppp

The global configuration command “aaa authentication ppp” can be used for designating one or multiple AAA authentication methods used for running serial interface of PPP. The “no” format of the command is used for closing authentication.

Syntas

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

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

Parameter

Parameter	Description
Default	It uses the authentication method list following the parameter as the default authentication method at the time of the user's login.
list-name	It is used to name the character string of authentication method list.
mehod1 [*method2...*]	It is one of the methods described in Form 3 at the least.

Default

If no default is set, the database of local users shall be examined for authentication. It has the same effect as the command below:

aaa authentication ppp default local

Command mode

global configuration mode

Explanation

The default list and naming list created by the command "aaa authentication ppp" are used in the command "ppp authentication". These lists contain four authentication methods at most. These authentication methods are used when the user connects the serial interface.

The list is created by the command "aaa authentication ppp list-name method", of which the keyword "list-name" is used for naming any character string of the list. The parameter "method" designates the specific authentication methods. These methods are used in the authentication process on the sequence of configuration. Four methods can be entered at most. The keywords of the methods is described in Form 3.

Only when the said authentication method feeds back error will other authentication methods be used. Should the said authentication method feed back the failure, no other authentication methods will be used. "none" shall be designated as the last method of the command line to ensure the success of authentication even if all the authentication methods feed back error.

Figuer 1-3 PPP Method of AAA Authentication

Key Word	Description
group	The server group is used for authentication.
group-restrict	The server group is used for authentication. But when the user designates a server, the server group is disabled.
local	The database of local user names is used for authentication.
local-case	The database of local user names is used for authentication (case sensitive for user name)

none	No authentication is made.
radius	RADIUS is used for authentication
tacacs+	TACACS+ is used for authentication.

Example

AAA authentication methods list named “TEST” is created in the following example for using the serial line of PPP. This authentication first tries connecting with TACACS+server. If error is fed back, the user will be allowed to access the network without authentication.

aaa authentication ppp TEST tacacs+ none

Relevant command

ppp authentication

1.1.4 aaa authentication password-prompt

The global configuration command “aaa authentication password-prompt” should be used for changing the text display prompting the user password input. The “no” format of the command can be employed for reusing the default prompt text of the password.

Syntas

aaa authentication password-prompt *text-string*

no aaa authentication password-prompt *text-string*

Parameter

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

Default

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

Command mode

global configuration mode

Explanation

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:

Relevant command

aaa authentication username-prompt

enable password

1.1.5 aaa authentication username-prompt

The global configuration command “aaa authentication username-prompt” can be used for changing the text display prompting the user name input. The “no” format of the command is used for restoring the default prompting character string of the user name.

Syntas

aaa authentication username-prompt *text-string*

no aaa authentication username-prompt *text-string*

Parameter

Parameter	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

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

Command mode

global configuration mode

Explanation

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 will change the prompt of username into the displayed character string.

aaa authentication username-prompt YourUsernam:

Relevant command

aaa authentication password-prompt

1.1.6 aaa authentication banner

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

Parameter

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

Default

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

User Access Verification

Command mode

Global configuration mode

Explanation

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 reaptedly at the end of the string, meaning the banner ends.

Example

The following example shows that the banner is modified to “Welcom to QTECH Router” when logging on:

aaa authentication banner “Welcome to QTECH Router”

Related command

aaa authentication fail-message

1.1.7 aaa authentication fail-message

To configure a personal banner when login fails, run **aaa authentication fail-message** in global mode.

aaa authentication fail-message *delimiter string delimiter*

no aaa authentication fail-message

Parameter

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

Default

If you do not define the banner for login failure, the default banner is:

Authentication failed!

Command mode

Global configuration mode

Explanation

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

Example

The following example shows that username prompt is changed to the following character string:

aaa authentication fail-message “See you later”

Related command

aaa authentication banner

1.1.8 aaa group server

The commands below are used to access to the configuration level of server group for supporting the configuration of AAA server group. The “no” format of the command is used to delete the configured server group.

Syntas

aaa group server radius *group-name*

no aaa group server radius *group-name*

Parameter

Parameter	Description
group-name	Character string of the name of the server group.

Default

no server Group

Command mode

global configuration mode

Explanation

Accessing to configuration level of server group by using the command, then adding the corresponding sever to the group.

Example

aaa group server radius radius-group

The said command is used for adding a radiusserver group named ““radius-group”.

Relevant command

server

1.1.9 server

The command is used for adding a server in an AAA server group. The “no” format of the command is used for deleting a server.

Syntas

server *A.B.C.D*

no server *A.B.C.D*

Parameter

Parameter	Description
A.B.C.D	IP address of server

Default

no server

Command mode

Server Group Configuration Mode

Explanation

20 different servers can be added to a server group at most.

Example

server 12.1.1.1

The above command is used for adding the server whose address is 12.1.1.1 to server group.

Relevant command

aaa group server

1.1.10 service password-encryption

To encrypt related passwords in the system, run service password-encryption. **service password-encryption**

no service password-encryption

Parameter

None

Default

Related passwords in the system is not encrypted when they are displayed.

Command mode

Global configuration mode

Explanation

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 display 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

router_config#service password-encryption

This command is used 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

1.1.11 username

The command can be used for adding the user to the database of local users, authentication of local method and authorization. The “no” format of the method can be used for deleting the corresponding user.

Syntas

username *username* [**password** { *password* | [**encryption-type**] *encrypted-password* }] [**trust-host** *ip_address]* [**user-maxlinks** *number*] [**callback-dialstring** *string*] [**callback-line** *line*] [**callback-rotary** *rotary*] [**nocallback-verify**] [**autocommand** *command*]

no username *username*

Parameter

Parameter	Description
username	Character String of User Name
password	The password corresponding to the user
password	Plaintext of character string of password
encryption-type	The type of password encryption
encrypted-password	The ciphertext of the password corresponding to the encryption type limited by “encryption-type”.
trust-host	The trust-host corresponding to the user.
ip_address	IP address of trust-host, the authentication can be passed only when the user logs in the router from the host.
user-maxlinks	The maximum links to the router, the same user can create at the same time (Statistic is made only to the user passing the local authentication.
number	The number of links created at the same time.
callback-dialstring	Callback the telephone number
string	Character string of telephone number
callback-line	The line used for callback
line	Line number
callback-rotary	Callback rotary configuration
rotary	rotary number
nocallback-verify	Callback is not verified.
autocommand	When the user logs in the router, the designated command will be executed automatically.
command	Automatic execution of character string of the command.

Default

No user

Command mode

global configuration mode

Explanation

When there is no password parameter, the password will be interpreted as null character string. The trust-host bundles up the user and specific host together. When the user logs in the router from another host, the user will have the “none” method to pass the authentication. “user-maxlinks” limits the number of dialogues the same user set up with the router at the same time. However, when a dialogue of the user is not authenticated by the local authentication method, the dialogue will not be included. The command “show users” can be used for examining the kind of authentication the users uses to pass.

The password of router configuration of Our Company contains no blank, namely at the time of using the command “enable password”, the blank shall not be entered when the plaintext of password needs to be entered directly.

Currently there are only two encryption-types supported by our router system. The parameters in the commands are 0 and 7 respectively. 0 stands for 0, meaning no encryption. The plaintext of password is entered directly in the following *encrypted-password.* This method has the same effect as the method of direct input of password parameter without adding encryption-type. 7 represents a kind of algorithm defined by Our Company for encrypting. The encrypted ciphertext of password is needed to be entered in the following *encrypted-password*. The ciphertext can be copied from other configuration files of the router.

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.

Relevant command

aaa authentication login

aaa authentication ppp

1.1.12 enable password

To configure the privilege-level password to authenticate the privileged user, run **enable password**. To cancel the privilege-level password, run **enable password [*level number*]**.

enable password { ***password*** | [**encryption-type**] ***encrypted-password*** } [***level*** *number*]

no enable password [***level*** *number*]

Parameter

Parameter	Description
password	Plain text of the password character string
encryption-type	Type of password encryption
encrypted-password and **encryption-type**	Cipher text of the password which corresponds to the limited encryption type
level	Privilege level
number	Value of the privilege level (1-15)

Default

There is no password by default.

Command mode

Global configuration mode

Explanation

The passwords configured for QTECH router 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 126 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.

encryption-type means the type of password encryption. Currently only two types, 0 and 7, are supported. **0** means that the data is not encrypted. The plain text of the password is directly entered for the parameter **encrypted-password**, which has the same result as the password is directly entered without adding the encryption-type. **7** means that an algorithm defined by QTECH is used for encryption. For the **encrypted-password** parameter, the encrypted password text need be entered, which can be copied from the configuration file of other routers.

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 routers.

Related command

aaa authentication enable default

service password-encryption

1.1.13 debug aaa authentication

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

debug aaa authentication

no debug aaa authentication

Parameter

None

Default

The debug information is shut down.

Command mode

EXEC

Explanation

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

Related command

debug aaa authorization

debug aaa accounting

1.1.14 show aaa users

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

show aaa users

Parameter

None

Default

None

Command mode

EXEC

Explanation

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

Example

#show aaa users

Port	User	Service	Duration	Peer-address
console 0	zjl QTEC	exec	04:14:03	unknown
vty 0	H	exec	00:12:24	172.16.20.120
serial2/1	admin	ppp(chap)	01:43:09	192.168.20.87

Domain	Explanation
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

1.2 AAA Authorization Configuration command

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.

1.2.1 aaa authorization

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.

Syntas

aaa authorization network {**default** | *list-name*} [*method1 [method2...*]]

no aaa authorization network

Parameter

Parameter	Description
network	The authorization of network type service
default	Default authorization methods list
list-name	The character string used for naming authentication methods list.
method1 [method2...]	One of the keywords listed in the form below.

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

Explanation

The command “aaa authorization” is used for opening 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 andTACACS+). 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.

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

Keyword of AAA Authorization:

Keyword	Description
Group	The server group is used for obtaining the authorization information
group-restrict	The server group is used for obtaining the authorization information. However, when the user has designated the server requested for use, the server group is disabled.
tacacs+	TACACS＋ is used for obtained authorization information.
if-authenticated	If the user passes the authorization, the user is allowed to access the function required.
none	Authorizing the pass of none condition.
local	The local database is used for authorization.
radius	RADIUS is used for obtaining authorization information.

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 network have_a_try radius local

Relevant command

aaa authentication

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.

1.3.1 aaa accounting

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 { **network** | **exec** | **connection**} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} **group** *groupname*

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

Parameter

Parameter	Description
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 router. 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
method1 *[method2...]*	Accounting method For more details, refer to *Accounting Configuration*.

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

Explanation

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

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

Explanation

See *Accounting Configuration*.

Related command

aaa accounting

1.3.3 aaa accounting suppress null-username

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

Explanation

See *Accounting Configuration*.

Related command

aaa accounting

Chapter 2 **RADIUS Commands**

2.1 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.

2.1.1 debug radius

The command “debug radius” can be executed for tracing RADIUS event or packet. The “no” format of the command can be used for closing debug information.

Syntas

debug radius {**event** | **packet**}

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

Parameter

Parameter	Description
event	Tracing RADIUS event
packet	Tracing RADIUS packet

Default

none

Command mode

Supervisor mode

Explanation

The command can be used for debugging network system to find out the cause of authentication failure.

Router#debug radius event

RADIUS:return message to aaa, Give me your username

RADIUS:return message to aaa, Give me your password

RADIUS:inital transmit access-request [4] to 192.168.20.126 1812 <length=70>

RADIUS:retransmit access-request [4] to 192.168.20.126 1812 <length=70>

RADIUS:retransmit access-request [4] to 192.168.20.126 1812 <length=70>

RADIUS:192.168.20.126 is dead to response [4]

RADIUS:Have tried all servers，return error to aaa.

Output Information	Explanation
Return packet to aaa, Give me your username	The username wantd
Return packet to aaa, Give me your password	The password corresponding to the username wanted.
inital transmit access-request [4] to 192.168.20.126 1812 <length=70>	The first authentication request is sent to the RADIUS server. The address of the server is 192.168.20.126, the port number is 1812, the length of packet is 70.
retransmit access-request [4] to 192.168.20.126 1812 <length=70>	Server does not echo the request and authentication request is retransmitted.
192.168.20.126 is dead to response [4]	After repeated retransmission, server is dead to response, the server is marked as dead.
Have tried all servers return error to ， aaa	The authentication is completed by using RADIUS and the error is returned.

Example

The following Example opens event trace of RADIUS.

debug radius event

2.1.2 ip radius source-interface

The global configuration command “ip radius source-interface” is used for compelling RADIUS to use IP address of the designated interface for all the packets transmitted by RADIUS. The “no” format of the command is used for restoring the default value.

Syntas

ip radius source-interface *interface-name*

no ip radius source-interface

Parameter

Parameter	Description

interface-name	RADIUS uses IP address of the interface for all RADIUS packet sent.

Default

The command has no default value designated by the manufacturer, i.e., the source IP address should be determined on the real condition.

Command mode

global configuration mode

Explanation

The command is used for selecting the IP address of an interface as the source address of sending out RADIUS packet. So long as the interface is under “up” state, the address will be used continuously. Thus, for each client accessing the network, RADIUS server only uses one IP address rather than maintaining an IP address list. The command is especially useful when the router has many interfaces and intends to ensure that all RADIUS packets coming from some specific router has the same IP address.

The designated interface shall have IP address related to the interface. If the designated interface does not have an IP address or is under a “down” state, RADIUS will restore to the default value. In order to avoid the case, IP address should be added to the interface and the interface shall be ensured under “up” state.

Example

The following Example allows RADIUS to use IP address of the interface s1/2 for all RADIUS packets used.

ip radius source-interface s1/2

Relevant command

ip tacacs source-interface

2.1.3 radius-server attribute

To designate some attributes to be transmitted during radius authentication and charging, run **radius-server attribute**. To cancel some designated attributes to be transmitted, run **no radius-server attribute**.

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

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

Parameter

Parameter	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.

Default

None

Command mode

Global configuration mode

Explanation

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

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.

Related command

None

2.1.4 radius-server challenge-noecho

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

Syntas

radius-server challenge-noecho

no radius-server challenge-noecho

Parameter

none

Default

The user data is shown under the Access-Challenge.

Command mode

global configuration mode

Explanation

none

Example

radius-server challenge-noecho

2.1.5 radius-server dead-time

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.

Syntas

radius-server dead-time *minutes*

no radius-server dead-time

Parameter

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

Default

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

Command mode

global configuration mode

Explanation

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 dead-time 5

Relevant command

radius server host

radius-server **retransmit**

radius-server **timeout**

2.1.6 radius-server host

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.

Syntas

radius server host *ip-address* [**auth-port** *port-number1*] [**acct-port** *port-number2*] **no radius server host** *ip-address*

Parameter

Parameter	Description
ip-address	*the ip 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. If the setting is 0, the host is not used for authentication.*
acct-port	*(optional item) Designating UDP destination port for accounting request.*
port-number2	*(optional item) The port number of accounting request. If the setting is 0, the host is not used for accounting.*

Default

Any RADIUS host is not designated.

Command mode

global configuration mode

Explanation

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 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 1.2.1.2 auth-port 12 acct-port 16

Relevant command

aaa authentication

radius key

tacacs server

username

2.1.7 radius-server optional-passwords

The global configuration command “radius-server optional-passwords” is used for verifying the username without checking password when RADIUS authentication request is transmitted to RADIUS server for the first time. The “no” format of the command can be used for restoring the default value.

Syntas

radius-server optional-passwords

no radius-server optional-passwords

parameter

none

Default

optional-password mode is not used.

Command mode

global configuration mode

Explanation

When the user enters login name, the authentication request will include the user name and zero length password. If the authentication request is accepted, the login authentication process is completed. If RADIUS server refuses the request, the server will prompt the password input. When the user enters the password, the second authentication will be tried. RADIUS server shall support the authentication of the user of no password so as to take advantage of this feature.

Example

The following Example configures the exclusion of user password when the first authentication request is transmitted.

radius-server optional-passwords

Relevant command

radius server host

2.1.8 radius-server key

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.

Syntas

radius-server key *string*

no radius-server key

Parameter

Parameter	Description
string	The secret key used for encrypting. The secret key shall match with the one used by RADIUS server.

Default

The secret key is a null character string.

Command mode

global configuration mode

Explanation

The entered secret key shall match with the one used by RADIUS server. All the zero space character is neglected. The secret key contains no space character.

Example

The following Example sets encryption key as “firstime”.

radius-server key firstime

Relevant command

radius server

tacacs server

username

2.1.9 radius-server retransmit

The global configuration command is used for designating the times of trial before abandoning some server. The “no” format of the command can be used for restoring default value.

Syntas

radius-server retransmit *retries*

no radius-server retransmit

Parameter

Parameter	Description
retries	The maximum times of repeated trial, the default value is 3 trials.

Default

3 trials

Command mode

global configuration mode

Explanation

The command is usually used together with the command “radius timeout”, indicating the time of the timeout of server response and the times of repeated trails after the timeout.

Example

The Example below designates the value of retrial of counter as 5.

radius retransmit 5

Relevant command

radius-server timeout

2.1.10 radius-server timeout

The global configuration command “radius-server timeout” is used for setting the time to wait for the server response to the router. The “no” format of the command is used for restoring default value.

Syntas

radius-server timeout *seconds*

no radius-server timeout

Parameter

Parameter	Description
seconds	Designating the timeout (unit: second), the default value is 5

	seconds.

Default

5 seconds

Command mode

global configuration mode

Explanation

The command is usually used together with the command “radius retransmit”.

Example

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

radius timeout 10

2.1.11 radius-server vsa send

The global configuration command “radius-server vsa send” can be used for configuring the router into the one that is identified and uses special attribute of manufacturer (VSA). The “no” format of the command can be used for restoring the default value.

Syntas

radius-server vsa send [accounting | authentication]

no radius-server vsa send [accounting | authentication]

Parameter

Parameter	Description
accounting	(optional item) The identified special attribute of the manufacturer is limited to the accounting attribute.
authentication	(optional item) The identified special attribute of the manufacturer is limited to the authentication attribute.

Default

VSA is not used.

Command mode

global configuration mode

explanation

IETF uses special attribute of manufacturer (VSA) (attribute 26) and designates the method for exchanging the special information of the manufacturer between the router and RADIUS server. VSA allows manufacturers to support their own extended attribute not suitable to universal purposes. The command “radius vsa send” enables the router to identify and use the special attribute of the manufacturer (VSA) of authentication and accounting. The keyword “accounting” is used in the command “radius vsa send” to limit the identified special attribute of the manufacturer to the attribute of accounting. The keyword “authentication” is used in the command “radius vsa send” to limit the identified special attribute of the manufacturer to the attribute of authentication.

Example

The Example below configures the router to enable it to identify and use the special accounting attribute of manufacturer.

radius-server vsa send accounting

Relevant command

radius server host

Chapter 3 **TACACS+ Commands**

3.1 TACACS+ Command

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.

3.1.1 debug tacacs

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.

Syntas

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

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

Parameter

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

Default

Closing debug information

Command mode

supervisor

Explanation

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

Relevant commands

none

3.1.2 ip tacacs source-interface

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

Syntas

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＋ packets.

Default

None

Command mode

global configuration mode

Explanation

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 s1/0 as source IP address of all TACACS+ packets.

ip tacacs source-interface s1/0

Relevant commands

ip radius source-interface

3.1.3 tacacs server

The global configuration command “tacacs server” is used for designating TACACS＋ server. The “no” format of the command is used for deleting the designated server.

Syntas

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

no tacacs serve *ip-address*

Parameter

Parameter	Description
ip-address	IP address of 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.

Default

No TACACS＋server is designated.

Command mode

global configuration mode

Explanation

Use multiple commands of “tacacs server” to designate multiple hosts and searching the hosts on the designated order. As some parameters of the commands of “tacacs server” will cover the global configuration set by the command “tacacs timeout” and “tacacs key”, the command can be used to configure the communication attribute of each TACACS+server exclusively so as to advance the security of the network.
Example

The Example below designates the negotiation between the router and TACACS+server whose IP address is 1.1.1.1 so as to make AAA authentication, and designates TCP service port number 51, sets the value of timeout 3 seconds. The encryption key is “a_secret”.

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

Relevant commands

tacacs key

tacacs timeout

3.1.4 tacacs key

The global configuration command “tacacs key” shall be used for setting the encryption key used by all communication process between the router and TACACS+server. The “no” format of the command is used for closing the encryption key.

Syntas

tacacs key key

no tacacs key

Parameter

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

Command mode

global configuration mode

Explanation

The command “tacacs key” shall be used for setting encryption key before TACACS+protocol is running. The entered secret key shall match with the one used by the service program of TACACS+. All the drive-head blanks are ignored and the secret key contains no blank.

Example

The example below sets encryption key as “testkey”:

tacacs key testkey

Relevant commands

tacacs server

3.1.5 tacacs timeout

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.

Syntas

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

Explanation

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 timeout 10
```

Relevant commands

tacacs server

Chapter 4 **IPSec Commands**

4.1 IPSec Command

This chapter describes the commands for IPSec configuration. IPSec provides the security for transmitting the sensitive information on the public network, such as Internet. The security solution provided by IPSec is very powerful and is based on the standards. As the supplement to the data confidentiality, IPSec also offers the service of data verification and anti-replay.

4.1.1 crypto nat

To enable the transparent NAT negotiation mode, run **crypto nat**.

crypto nat

no crypto nat

Parameter

None

Default

shutdown state

Command mode

EXEC

Explanation

If the command has the **nat** parameter concluded, the negotiation packet contains some information about NAT, which makes the negotiation process insecure. Generally, the **nat** parameter is excluded. It is included by the command only when it is necessary. The **nat** information is not affected during the negotiation process, which can be accepted forever.

When the **nat** information exists, the IP authentication cannot be approved. In this case, the ID authentication need be adopted. You can configure the ID in the encrypted mapping table.

Example

If the **nat** device exists, open the **nat** penetrating negotiation mode.

crypto nat

Related command

crypto identification *word*

4.1.2 crypto identification

To configure an ID type and an ID value, run the **crypto identification word** command in ID configuration mode.

crypto identification *word*

no crypto identification

Parameter

Parameter	Description
word	ID configuration name

Default

The default local ID configuration exists.

Command mode

EXEC

Explanation

The ID authentication domain is used at the first phase of the IKE configuration. By default, the IP addresses at both channel ends serve as the content of the ID authentication domain. The ID content can be specified. Currently, only the **dn** and **fqdn** types are supported.

The detailed configuration procedure is described at later parts.

Example

The following command is used to configure the ID of the negotiation object.

crypto identification abc

Related command

fqdn

dn

4.1.3 fqdn

To set an ID for the **fqdn** type, run **fqdn**.

fqdn *word*

no fqdn

Parameter

Parameter	Description
Word	ID content

Default

None

Command mode

ID configuration mode

Explanation

It is used to configure an ID of the fqdn type.

Example

fqdn abc

Related command

dn

4.1.4 dn

To set an ID of the **dn** type, run **dn**.

dn *word*

no dn

Parameter

Parameter	Description
Word	ID content

Default

None

Command mode

ID configuration mode

Explanation

It is used to configure an ID of the **dn** type.

Example

dn abc

Related command

4.1.5 fqdnclear crypto sa

The command “clear crypto sa” is used for deleting the related IPSec security association database.

Syntas

clear crypto sa[**peer** *ip-address*| **map** *map-name*]

Parameter

Parameter	Description
peer	Keyword IP address of the opposite terminal.
ip-address	Designating IP address of the opposite terminal.
map	Keyword the name of the encrypted map set.
map-name	Designating the name of the encrypted map set.

Default

If the keyword of peer, map and others are not used, all the IPSec security association

will be deleted.

Command mode

Supervisor mode

Explanation

The command is used for clearing (deleting) IPSec security association. If security association are set up through IKE, they will be deleted. The later IPSec communication requires a re-negotiation of new security association (When IKE is used, IPSec security association is set up only in the time of need)

If the security association is set up through manual work, the security association will be deleted and will re-established.

If the keyword of peer, map and others are not used, all IPSec security association will be deleted. The use of keyword peer will delete all IPSec security association of designated address of the opposite terminal. The use of keyword map will delete all IPSec security association created by encrypted map set. All the security association can be re-established by using the command “clear crypto sa”. So these security association can use the latest configuration settings. Under the circumstance of setting up security association by manual work, the command “clear crypto sa” shall be used before the amendment to map set takes effect

If the router is processing IPSec communication, the contents that are most vulnerable to the effect in the security association database had better be cleared in a purpose of avoid the sudden interruption of the on-going IPSec communication. It shall be noted that the command only clears IPSec security association. The command “clear crypto isakmp” shall be used for clearing IKE state.

Example

The Example below clears all Ipsec security association on the router.

clear crypto sa

Relevant command

clear crypto isakmp

4.1.6 crypto dynamic-map

The global configuration command “crypto dynamic-map” can be used for creating or amending a dynamic encrypted map and entering into the configuration status of dynamic encrypted map. The “no” format of the command can be used for deleting a dynamic encrypted map or set.

Syntas

crypto dynamic-map *map-name*

no crypto dynamic-map *map-name*

Parameter

Parameter	Description
map-name	The name of dynamic encrypted map set

Default

dynamic encrypted map does not exist.

Command mode

global configuration mode. The command is used for entering into the configuration status of dynamic encrypted map.

Explanation

The command is used for creating a new dynamic encrypted map or amending the existing dynamic encrypted map.

The functions of dynamic encrypted map and common encrypted map are similar. The major differences lies in:

IP address of the opposite terminal does not need to be set in the dynamic encrypted map and allows IPSec equipment of any address to negotiate, this function can be used for supporting the connection with the mobile users. While common encrypted map shall designate IP address of the opposite terminal and only allows IPSec of the address to negotiate. IP address can be set in dynamic encrypted map. Under such circumstance, the dynamic encrypted map basically equals to the common encrypted map.

Example

The example below shows the configuration needed for the minimum encrypted map when IKE is used for establishing security association.

```
crypto dynamic-map aaa
match address aaa
set transform-set one
```

Relevant command

crypto map (global configuration)

match address

set peer

set pfs

set security-association lifetime

set transform-set

show crypto map

4.1.7 crypto ipsec secure

Designating the local router whether it should receive non-IPSec packet or incorrect IPSec packet or not.

Syntas

crypto ipsec secure

no crypto ipsec secure

Parameter

None

Default

Non-IPSec packet or incorrect IPSec packet is allowed to pass.

Command mode

global configuration mode.

Explanation

When packet passes and the user-defined rules are configured and if the packet is not IPSec packet or is incorrect IPSec packet, the router will process the packet as usual in the event that the option is not set at the time. If the option is set at the time, the router will abandon the packet.

Example

The example below sets the option of the router.

crypto ipsec secure

Relevant command

crypto map

4.1.8 crypto ipsec transform-set

The global configuration command “crypto ipsec transform-set” is used for defining a ipsec transform set---a feasible mix of security protocol and algorithm. The “no” format of the command can be used for deleting a transform set.

Syntas

crypto ipsec transform-set *transform-set-name*

no crypto ipsec transform-set *transform-set-name*

Parameter

Parameter	Description
transform-set-name	Designating the name of transform set that is to be created (or amended).

Default

None

Command mode

global configuration mode .The command is executed for entering the encryption transform configuration status.

Explanation

Transform set is the mix of security protocols, algorithm and other settings of communications subject to IPSec protection.

The multiple sets can be configured the none or multiple sets can be designated in the encrypted map. The transform set defined in the encrypted map is used for negotiating IPSec security association with a view to protecting the packets of access list set by the matched encrypted map. During the negotiation, the two sides search for the same transform set available to the two sides. When such set is found, the set will be selected as a part of IPSec association of two sides that is to be used on the protected communication.

If IKE is not used for setting up security association, a sole transform set shall be designated. The set shall have a negotiation.

Only after the transform set is defined by using the command, the transform set can be set in the encrypted map.

The command “transform-type” can be used for configuring the transform type.

Example

The example below defines a transform set.

crypto ipsec transform-set one

transform-type esp-des esp-sha-hmac

Relevant command

mode

transform-type

set transform-set

show crypto ipsec transform-set

4.1.9 crypto ipsec card-transform-set

The transform-set defined by the command adopts the hardware encryption card of the national password management office to encrypt the data.

crypto ipsec card-transform-set *transform-set-name*

no crypto ipsec card-transform-set *transform-set-name*

Parameter

Parameter	Description
transform-set-name	Name of the specified to-be-established/modified transformation set

Default

None

Command mode

Encrypted transformation configuration mode after the command is run.

Explanation

The transformation set is a combination of security protocol, algorithm and other settings about IPSec-protected communication.

You can configure multiple transformation sets and then specify one or multiple transformation sets in the encrypted mapping table. The transformation set defined in the encrypted mapping table is used to negotiate the IPSec security ally to protect the message that matches the access list set by the encrypted mapping table. During the negotiation, the two negotiation sides will find a same transformation set. When such a

transformation set is detected, the set will be selected and used at the protected communication as part of the two-sided IPSec security ally.

If the security ally is not established through IKE, a unique transformation set must be specified. However, the transformation set need not be negotiated.

Only after the transformation set is defined through the **crypto ipsec transform-set** command can it be set in the encrypted mapping table.

You can run **transform-type** to configure the tranformation type.

Example

The following example shows a transformation set is defined.

crypto ipsec card-transform-set one

transform-type esp-nca esp-sha-hmac

Related command

mode

transform-type

set transform-set

show crypto ipsec transform-set

4.1.10 crypto map (global configuration)

The global configuration command can be used for creating or amending an encrypted map and entering into the configuration status of encrypted map. The “no” format of the command can be used for deleting an encrypted map or set.

Syntas

crypto map *map-name seq-num* **ipsec-manual**

crypto map *map-name seq-num* **ipsec-isakmp**

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

no crypto map *map-name seq-num*

Parameter

Parameter	Description
map-name	The name of encrypted map set
seq-num	Serial number of encrypted map. The detailed explanation of how to use the parameter can be referred to the part of “Direction for Use”.

ipsec-manual	IPSec Security Association is set up through manual work for protecting the communication designated by the encrypted map.
ipsec-isakmp	IPSec Security Association is set up through IKE for protecting the communication designated by the encrypted map.
dynamic-map-name	The encrypted map is used as the name of dynamic encrypted map that serves as templete.

Default

The encrypted map does not exist.

Command mode

global configuration mode .When there is no dynamic and its parameter, the command shall be used for entering into the configuration status of encrypted map.

Explanation

The command is used for creating a new encrypted map or amending an existing encrypted map.

After an encrypted map is created, the parameter designated under global configuration mode cannot be changed because these parameters decide which commands can be used in the configuration status of encrypted map. For example, Once a map is created as ipsec-isakmp, it cannot be changed into ipsec-manual. It shall be deleted and changed into ipsec-manual under the configuration status of the encrypted map. After the encrypted map is defined, the command “crypto map （interface configuration）can be used for applying the encrypted map set to the interface.

The function of the encrypted map

The encrypted map bears two functions: Filtrating and classifying the communication that needs to be protected and defining the policy of communication. The encrypted map of IPSec links the definitions below together:

The communications that should be protected.

The opposite terminal of IPSec accessible to the data under protection can set up a security association with the local router.

How to manage and use secret key and security association (or when IKE is not used, what is secret key)

The multiple encrypted maps with the same map name forms a encrypted map set.

The encrypted map set is the gathering composed of the encrypted maps, of which each map has different seq- num and same map-name. Therefore, for the given interface, some security policy can be adopted to the communication transmitted to the opposite terminal of IPSec. The different security policies shall be adopted to other communications transmitted to the same or the different opposite terminals of IPSec. To this end, two encrypted maps shall be created, each map has the same map-name, but has different seq-num.

Seq-num parameter

The numerical value of seq-num cannot be defined at will. The numerical value is used for sequencing the multiple encrypted map in an encrypted map set. The encrypted map with small seq-num is judged before the with big seq-num, which means that the smaller the num numerical value is, the more priority the mapping has.

For instance, Here is the assumption that the encrypted map set contains three encrypted maps: aaa 10，aaa 20 and aaa 30. The encrypted map set named aaa is used on the interface Serial 0. When the communication passes through the interface Serial 0, it shall be judged by aaa 10. If the communication matches with a permit in the extended access list designated by aaa 10, the communication will be processed on the policy defined in aaa 10 (including the IPSec security association established when necessary). If the communication does not matches with aaa 10 access list, aaa 20 will be used, the aaa 30 will judge the communication, till the communication matches with a permit sentence in a map (if the communication does not match with the permit sentence in any encrypted map, the communication will be transmitted directly without any IPSec protection.

Example

The following example shows the required minimum configuration for the encrypted map when the security association is set up through IKE.

```
crypto map aaa 10 ipsec-isakmp
   match address aaa
set transform-set one
set peer 192.2.2.1
```

The following example shows the required minimum configuration for the encrypted map when the security association is set up through dynamic encrypted map.

```
crypto dynamic-map aaa
   match address aaa
set transform-set one
crypto map bbb 10 ipsec-isakmp dynamic-map aaa
```

The following example shows the required minimum configuration for the encrypted map when the security association is set up through manual work.

```
crypto transform-set one transform-
type ah-md5-hmac esp-des crypto
map aaa 10 ipsec-manual match
address aaa
set transform-set one
set peer 192.2.2.1
set security-association inbound ah 300 98765432109876543210987654
set security-association outbound ah 300 fedcbafedcbafedcfedcbafedcbafedc set
security-association inbound esp 300 cipher 0123456789012345
set security-association outbound esp 300 cipher abcedfabcdefabcd
```

Relevant command

crypto map (interface configuration)

crypto map local-address

match address

set peer

set pfs

set security-association lifetime

set transform-set

show crypto map

4.1.11 crypto map (interface configuration)

The command “crypto map” can be used for applying the encrypted map set defined in advance to the interface. The “no” format of the command can be used for removing the encrypted map set from an interface.

Syntas

crypto map *map-name*

no crypto map

Parameter

Parameter	Description
map-name	The name of the set of encrypted maps

Default

The encrypted map is not configured on the interface.

Command mode

Interface Configuration mode

Explanation

The command is used for applying the encrypted map set to the interface. An encrypted map set shall be configured before the interface is able to provide IPSec service. Only an encrypted map set can be set for an interface. If multiple encrypted maps have the same map-name and different seq-num, they will be in the same set

and will applied to the same interface. The encrypted map with the smaller Seq-num has the more priority and will be judged beforehand. An encrypted map set is likely to contain the mix of the encrypted maps of ipsec-isakmp and ipsec-manual.

Example

The example below contributes the encrypted map set aaa to the interface S0. When the packet passes through the interface S0, all the encrypted maps in “mymap” set will be used for judging the packet. When the outbound packet matches with the access list corresponding to a linkage in the encrypted maps of “mymap”, the linkage based on the security association (IPSec supposed) configured by the encrypted map will be established (if there is no existing security association).

```
interface s0
crypto map aaa
```

Relevant command

crypto map (global configuration）

crypto map local-address

show crypto map

4.1.12 crypto map local-address

The command “crypto map local-address” can be used for designating an interface identifier and designating the identifier to be used for IPSec communication in the encrypted map. The “no” format of the command can be used for deleting the command from the configuration.

Syntas

crypto map *map-name* **local-address** *interface-id*

no crypto map *map-name* **local-address**

Parameter

Parameter	Description
map-name	The name of the encrypted map set
interface-id	Designating the interface identifier used by the encrypted map set.

Default

none

Command mode

global configuration mode

Explanation

If the command is configured, the local terminal address of IPSec of the encrypted map in the encrypted map set uses IP address of the designated interface

Example

none

Relevant command

crypto map (interface configuration)

4.1.13 debug crypto packet

In the course of process IPSec, the command is used for checking the error information resulting from the upper-layer data processing by IPSec.

Syntas

debug crypto packet

Parameter

none

Default

The related information is not shown under default status.

Command mode

Supervisor mode

Explanation

Some important and frequent-occurring information related to IPSec processing is shown in the list below.

Shown Information	Connotation of Information

rec'd IPSEC packet from IPADDR has invalid spi.	Spi value of outbound of the opposite terminal is different from the one of inbound of local terminal, or the configuration policy of configuration is different (esp, ah)
packet missing policy.	The configuration policy of outbound of the opposite terminal is different from the one of the local terminal (esp、ah)
rec'd IPSEC packet from IPADDR has bad pading.	The encryption key of outbound of the opposite terminal is different from the one of inbound of local terminal.
rec'd IPSEC packet mac verify failed.	ESP or AH verification secret key of outbound of the opposite terminal is different from the one of inbound of local terminal.
rec'd IPSEC packet from IPADDR to IPADDR does not agree with policy.	The packet processed by IPSec does not agree with the corresponding access-list. The configuration of access-list of Sub-MAP has problem.

Relevant command

show crypto ipsec sa

debug crypto isakmp

4.1.14 match address

The command “match address” can be used for designating an extended access list for an encrypted map. The “no” format of the command can be used for canceling the set extended access list from an encrypted map.

Syntas

match address *access-list-name*

no match address *access-list-name*

Parameter

Parameter	Description
access-list-name	Encryption access list. This name shall match with the name of the configured access list.

Default

Any access list is configured to the encrypted map.

Command mode

The configuration mode of the encrypted map

Explanation

The command is a must for all the encrypted maps.

The command is used for contributing the extended access list to an encrypted map. The command “ip access-list extended” is used for defining this access list.

The extended access list designated by the command is used by IPSec for judging which communication should be protected through encryption and which communications shall not be protected through encryption (The communication allowed by the access list will be protected and the communications refused by the access list will be not be protected in the corresponding encrypted map).

Notes:

The encrypted access list is not used for deciding whether the communication is allowed to pass some interface. The job is done by the access list that works on the interface.

The encrypted access list designated by the command is used for judging inbound communication and is also used for judging outbound communication. The encrypted access list corresponding to the encrypted map of interface will make judgment on the outbound communication to decide whether the communication should be got under encrypted protection and deciding the encryption policy employed if so (the communication configures a permit). After passing the examination of common access list on the interface, the inbound communication will be judged by the encrypted access list designated by the encrypted map set of the interface to determine whether the communication should be got under encryption protection and to decide which encryption policy should be adopted for protecting the communication (In the case of applying IPSec, the unprotected communication will be abandoned because it should be protected by IPSec.).

Example

The following example is the required minimum configuration of encrypted map created by IKE.

```
crypto map aaa 100 ipsec-isakmp
match address aaa
set transform-set one
set peer 192.2.2.1
```

Relevant command

crypto map(global configuration)

crypto map(interface configuration)

crypto map local-address

ip access-list extended

set peer

set pfs

set security-association lifetime

set transform-set

show crypto map

4.1.15 mode

The command of encryption transform configuration “mode” is used for changing the mode of a transform set. The “no” format of the command can be used for restoring the mode to the default value of tunnel mode.

Syntas

mode {**tunnel** | **transport**}

no mode

Parameter

Parameter	Description
tunnel|**transport**	Designating the mode of a transform set: tunnel mode or transport mode. If tunnel and transport are not designated, the default value (tunnel mode) will be used.

Default

Tunnel Mode

Command mode

Configuration mode of Encryption Transform

Explanation

The command is used for changing transform mode. Only when the message that is to be protected and two terminals of IPSec have the same IP address value (such kind of communication can be encapsulated under both tunnel mode and transport mode), the setting will be effective and will be ineffective for all the other communications (all the other communications are encapsulated under tunnel mode).

If the communication to be protected and two terminals of IPSec have the same IP address and the transport mode is designated, the router will apply for transport mode during the negotiation. Both transport mode and tunnel mode can be accepted. If tunnel mode is designated, the router will apply for tunnel mode and only the tunnel mode can be accepted.

After defining the transform set, the configuration status of encryption transform will follow. Under the configuration status, the mode can be changed into tunnel mode or transport mode.

If the mode is not set at the time of defining transform set and the mode of the transform set needs to be changed later, the transform set shall be re-accessed and its mode shall be changed.

If the command is used for changing the mode, the change will only affect the setup of the subsequent IPSec security association of the encrypted map designating the transform set. If the configuration of the transform set is needed to take effect as soon as possible, the partial or whole database of security association can be cleared. The more details can be secured by referring to the command “clear crypto sa”.

Tunnel Mode:

Under tunnel mode, the whole original IP message will be protected (encryption, verification or both two) and is encapsulated by IPSec (ESP, AH or both two). Then the new IP head will be added to the message, the IP head designates IPSec source and destination address.

Any IP communication can be transmitted by tunnel mode. If IPSec is used for protecting the communication of the host linked to the back of two terminals of IPSec, the tunnel mode shall be used.

Under transport mode, only the effective load (data) of IP subgroup is protected (encryption, verification or both two) and is encapsulated by IPSec (ESP, Ah or both two). The original IP message head remains unchanged and is not protected by IPSec. Only when the source of IP subgroup to be protected and destination address are the two terminals of IPSec, the transport mode is used. For instance, the transport mode can be used for protecting router management communication. Designating the transport mode in the application enables the router to negotiate with the remote terminal for deciding the transport mode or tunnel mode should be used.

Example

The example below defines a transform set and changes the mode into transport mode.

```
router_config# crypto ipsec transform-set one
router_config_crypto_trans#transform-type esp-des esp-sha-
hmac router_config_crypto_trans # mode transport
router_config_crypto_trans # exit
router_config#
```

Relevant command

crypto ipsec transform-set

4.1.16 id

To specify the ID in the encrypted mapping table, run **id *name***.

id *name*

no id *name*

Parameter

Parameter	Description
Name	ID configuration name

Default

The peer ID of IPSec is not specified.

Command mode

Configuration mode of the encrypted mapping table

Explanation

It is used to specify a peer IPSec ID for the encrypted mapping table. For all encrypted mapping tables, the command is necessary. One encrypted mapping table can specify only one IPSec peer ID. To change the peer, you just need to specify a new peer. The original settings will be out of effect.

Example

The following example shows the encrypted mapping table configuration when IKE is used to establish the security ally.

```
crypto map aaa 100 ipsec-isakmp
id abc
```

Related command

crypto map(global configuration)

crypto map(interface configuration)

crypto map local-address

match address

set peer

set pfs

set security-association lifetime

set transform-set

show crypto map

4.1.17 set peer

The configuration command of encrypted map “set peer” can be used for designating the opposite terminal of IPSec in the encrypted map. The “no” format of the command can be used for deleting the opposite terminal of IPSec from the encrypted map.

Syntas

set peer *ip-address*

no set peer *ip-address*

Parameter

Parameter	Description
ip-address	The opposite terminal of IPSec designated by IP address.

Default

The opposite terminal of IPSec is not designated under default state.

Command mode

Configuration mode of Encrypted Map

Explanation

The command is used for designating an opposite terminal of IPSec for the encrypted map. The command is a must for all the encrypted maps. One encrypted map can only designate one opposite terminal of IPSec. If the opposite terminal needs to changed, the new opposite terminal can be designated, which will cover the original settings.

Example

The example below shows the configuration of an encrypted map at the time IKE is used for creating a security association.

```
crypto map aaa 100 ipsec-isakmp
match address aaa
set transform-set one
set peer 192.2.2.1
```

Relevant command

crypto map(global configuration)

crypto map(interface configuration)

crypto map local-

address match address

set pfs

set security-association lifetime

set transform-set

show crypto map

4.1.18 set pfs

When the new security association is applied for the encrypted map, IPSec shall be designated to applying for perfect forward system (PFS), or when the application for setting up new security association is received, IPSec will demand PFS that the configuration command of encrypted map “set pfs” can be used. The “no” format of the command can be used for determining that IPSec will not apply for PFS

Syntas

set pfs [**group1**|**group2**]

no set pfs

Parameter

Parameter	Description
group1	When new Diffle-Hellman exchange is organized, the designated IPSec will use 768-digit Diffle-Hellman group.
group2	When new Diffle-Hellman exchange is organized, the designated IPSec will use 1024-digit Diffle-Hellman group.

Default

Under default state, PFS is not required.

Command mode

The configuration mode of encrypted map

Explanation

The command is applicable only to the encrypted map of ipsec-isakmp.

During the negotiation period, the command enables IPSec to apply for new security association for the encrypted map and PFS simultaneously. When the local terminal starts negotiation and local configuration designates the use of PFS, the opposite

terminals shall organize PFS exchange, otherwise the negotiation will fail. If local configuration does not designate a group, the local router will suggest the use of default value group1 and either group 1 or group 2 provided by the opposite terminal will be accepted. If local configuration designates group 2, the opposite terminal shall provide this group, otherwise the negotiation will fail. If local configuration does not designate PFS, the local router will accept PFS provided by the opposite terminal.

PFS adds the security of another level. If one secret key is attacked or decrypted, only the data that is transmitted under this secret key will be threatened. Without PFS, the data transmitted under other secret key is likely to be threatened. Under the case of using PFS, a new Diffle-Helman exchange will be started at the time of negotiating new security association (this exchange takes extra time for processing).

1024-bite Diffle-Hellman group, namely group 2, offers more security than group 1 does. But it takes more time for processing.

Example

The following example designates that PFS should be used at any time when encrypted map aaa 100 negotiates new security association.

```
crypto map aaa 100 ipsec-isakmp
set pfs group2
```

Relevant command

crypto map (global configuration)

crypto map (interface configuration)

crypto map local-address

match address

set peer

set security-association lifetime

set transform-set

show crypto map

4.1.19 set security-association lifetime

The configuration command of encrypted map “Set security-association lifetime” can be used for setting lifetime value for an encrypted map (this value is used for negotiating IPSec security association). The “no” format of the command can be used for restoring the lifetime value of an encrypted map to the default value.

Syntas

set security-association lifetime [**seconds** *seconds* | **kilobytes** *kilobytes*]

no set security-association lifetime [**seconds** | **kilobytes**]

Parameter

Parameter	Description
seconds *seconds*	Designating the surviving seconds of a security association before the timeout terminates.
kilobytes *kilobytes*	The communication traffic that can be transmitted by using this security association before the timeout of a security association occurs (calculated on kilobyte)

Default

The security association of encrypted map is negotiated on the default lifetime value.

Default timeout value is 3600 seconds (1 hour), the communication traffic under default state is 4,608,000 kilobyte.

Command mode

Configuration status of encrypted map

Explanation

The command is applicable only to the ipsec-isakmp encrypted map.

IPSec security association uses the shared secret keys. These secret keys and their corresponding security association overtimes simultaneously. Given the assumption that the specified encrypted map has been configured with new lifetime when the router applies for new security association in the negotiation of security association, it will use its own lifetime value of encrypted map in the application made to the opposite terminal and use the value as the lifetime value of new security association. When the router receives the application for negotiation transmitted from the opposite terminal, it will take the smaller one of the lifetime values that are suggested by the opposite terminal and configured by the local router respectively as the lifetime of new security association.

The lifetime can be classified into two: one is the seconds lifetime, the other is kilobyte lifetime. Either one of the two lifecycles expires first, the security association will overtime.

The format of the command “set security-association lifetime seconds” can be used for changing seconds lifetime that designates that security association and secret key overtimes after the given seconds.

The format of the command “set security-association lifetimekilobytes” can be used for changing the kilobyte lifetime that designates that security association and secret key overtimes when the communication traffic (calculated on KB) encrypted by the secret key of security association reaches a set amount.

The shorter the lifetime value is, the more difficult the secret key is attacked or decrypted as the data available to the attacker is less. However, the shorter the lifetime is, the more working time CPU takes for establishing new security association.

The lifetime value will be ignored at the time of setting up security association through manual work (The encrypted map of ipsec-manual is used for creating security association).

How lifetime works :

Given the assumption that the specified encrypted map is not configured with new lifetime, when the router applies for new security association, it will use the default lifetime value in the application made to the opposite terminal and will use the value as lifetime value of new security association. When the router receives the application for negotiation transmitted from the opposite terminal, it will take the smaller one of the lifetime values that are suggested by the opposite terminal and configured by the local router respectively as the lifetime value of new security association.

After a period of time (designated by the keyword “seconds”), a given byte of communication traffic is transmitted. Either of the said two events occurs first, the security association (and corresponding secret key) will overtime.

New security association starts negotiation before the lifetime limit of original security association is hit so as to ensure a new security association available when the original security association overtimes. The new security association starts negotiation 30 seconds in advance of the overtime of seconds lifetime or when the communication traffic transmitted through the tunnel has 256 KB away from kilobytes lifetime (based on the sequence of the occurrence of the events)

If no communication passes through the tunnel during the whole lifetime of a security association, the negotiation of new security association will be carried out when this security association overtimes. Correspondingly, the negotiation of new security association will be conducted only when IPSec gains a subgroup that shall be protected.

Example

This example of encrypted map sets the shorter lifetime value because the secret key of security association belonging to the encrypted map is likely to be stolen. Kilobyte lifetime value remains unchanged as the communication traffic sharing these security association is not so large. The seconds lifetime value is shortened to 1800 seconds (30 minutes).

```
crypto map aaa 100 ipsec-isakmp
set security-association lifetime seconds 1800
```

Relevant command

crypto map (global configuration)

crypto map (interface configuration)

crypto map local-address

match address

set peer

set pfs

set transform-set

show crypto map

4.1.20 set security-association {inbound|outbound}

The configuration command of encrypted map “set” can be used for designating secret key of IPSec through manual work in the encrypted map. The “no” format of the command can be used for deleting the secret key of IPSec from the encrypted map. The command is applicable only to the encrypted map of ipsec-manual.

Syntas

set security-association {inbound|outbound} ah *spi hex-key-string*

set security-association {inbound|outbound} esp *spi* **[cipher** *hex-key-string***] [authenticator** *hex-key-string***]**

no set security-association {inbound|outbound} ah

no set security-association {inbound|outbound} esp

Parameter

Parameter	Description
inbound	Setting secret key of IPSec of message (both the inbound message and outbound message shall be set).
Outbound	Setting secret key of IPSec of message (both the inbound message and outbound message shall be set).
Ah	Setting secret key of IPSec for AH protocol. Only when the transform set of this encrypted map includes AH transform, it works.
Esp	Setting secret key of IPSec for ESP protocol. Only when the transform set of this encrypted map includes ESP transform, it works.
spi	Security parameter index (SPI) is used for identifying a security association exclusively. SPI is a number give at random between 256 to 4,294,967,295（FFFFFFFF）. The same SPI can be given to the security association with two directions (inbound and outbound) and two protocols (AH, ESP). The sole SPI value shall be used for a mix with given destination address/protocol. Under the case of inbound, the destination address is the address of local router. Under the case of outbound, the destination address is the address of the opposite terminal.
hex-key-string	Secret key is entered in the format of hex. It is a random hex character string with a length of 8, 16, 20 or 24 bytes. If the transform set of the encrypted maps includes DES algorithm, each secret needs at least 8

	bytes. If the transform set of the encrypted maps includes 3DES algorithm, each secret needs at least 24 bytes. If the transform set of the encrypted maps includes MD5 algorithm, each secret needs at least 16 bytes. If the transform set of the encrypted maps includes SHA algorithm, each secret needs at least 20 bytes. The secret key exceeding the said lengths will be truncated simply.
cipher	Indicating this character string of secret key is the key of ESP encryption transform.
authenticator	(optional) indicating this character string of secret key is the key of ESP verification transform. This parameter is needed only when the transform set of this encrypted map includes ESP verification algorithm.

Default

Any secret key of IPSec is not defined under default state.

Command mode

The configuration mode of encrypted map

Explanation

The command can be used for designating secret key of IPSec for those security association created by the encrypted map of ipsec-manual (the encrypted map of ipsec-isakmp, security association and corresponding secret key is created through automatically through IKE negotiation.).

If the transform set of encrypted map includes AH protocol, the secret key of IPSe shall be defined for both outbound communication and inbound communication of AH. If the transform set of encrypted map includes the encrypted protocol of ESP, the secret key of IPSe shall be defined for both outbound communication and inbound communication of ESP encryption. If the transform set of encrypted map includes ESP verification protocol, the secret key of IPSe shall be defined for both outbound communication and inbound communication of ESP verification.

When multiple secret keys of IPSec is defined for an encrypted map, the same SPI number can be given to all the secret keys. SPI is used for identifying the security association corresponding to the encrypted map. However, not all the given value of SPI have the same randomness. The same SPI value shall be given only once for ensuring the mix of the same destination address /protocol.

The security association created by this command will not overtime (it is different from the security association created by IKE).

The secret key of local terminal shall match with the one of the opposite terminal. If the secret key is changed, the security association using the secret key will be deleted or re-added.

Example

The example below is the encrypted map of security association created through manual work. The transform set one includes only one AH protocol.

```
crypto ipsec transform-set one
transform-set ah-md5-hmac
crypto map aaa 100 ipsec-manual
match address aaa
set transform-set one
set peer 192.2.2.1
set security-association inbound ah 300 11111111111111111111111111111111
set security-association outbound ah 300 22222222222222222222222222222222
```

The example below is the encrypted map of security association created through manual work. The transform set one includes only one AH protocol and one ESP protocol. So both inbound and outbound communication of AH and ESP need configuring secret keys. This transform set includes the encryption of ESP and verification exchange. The keyword of cipher and authenticator should be used for creating secret key for these two transforms.

```
crypto ipsec transform-set one
transform-type ah-sha-hmac esp-des esp-sha-
hmac crypto map aaa 100 ipsec-manual
match address aaa
set transform-set one
set peer 192.2.2.1
set association inbound ah 300 98765432109876543210987654321098765432 10
set security-association outbound ah 300
fedcbafedcbafedcbafedcbafedcbafedcbafedcba fedc
set security-association inbound esp 300 cipher 0123456789012345
authenticator 00001111222233334444555566667777788889999
set security-association outbound esp 300 cipher abcdefabcdefabcd
authenticator 99998888777766665555444433332222111100 00
```

Relevant command

crypto map(global configuration)

crypto map(interface configuration)

crypto map local-address

match address

set peer

set transform-set

show crypto map

4.1.21 set transform-set

The configuration command of encrypted map of set transform-set can be used for designating the transform set used by the encrypted map. The “no” format of the command can be used for removing all transform sets from the encrypted map.

Syntas

set transform-set *transform-set-name1 [transform-set-name2...transform-set-name6]*

no set transform-set

Parameter

transform-set-name: The name of transform set. Only one transform set can be designated for encrypted map of ipsec-manual. Less than or equal to six transform set sets can be designated for ipsec-isakmp.

Default

Any transform set is included under default state.

Command mode

Configuration status of encrypted map

Explanation

The command is a must for all the encrypted maps.

The command is used for designating the transform sets that will be contained in an encrypted map

The command can be used for listing multiple transform sets for encrypted map of ipsec-isakmp. The transform set with top priority will be listed first.

If local router starts negotiation, the transform set will be provided to the opposite terminal on the sequence designated in the encrypted map. If the opposite terminal starts negotiation, the local router will accept the first matchable transform.

The first machable transform set found at the two terminals will be used for creating security association. If no match item is found, IPSec will not set up security association. The message will be abandoned because no security association protect these communications.

The sole transform set can be designated for the encrypted map of ipsec-manual. If this transform set is not able to match with the one of encrypted map of the opposite terminal, the two terminals of IPSec cannot communicate normally as they use different rules for protecting communication.

If the content of transform set needs to be changed, the content of the transform set shall be reset to cover the old one. This change will not affect the existing security association but will be used for creating new security association. If the change is needed to take effect as soon as possible, the command “clear crypto sa” can be used for deleting the whole or partial content of security association database.

Any transform set containing in an encrypted map shall be defined first by the command “crypto ipsec transform-set”.

Example

The example below defines two transform sets and designating them to be used in a same encrypted map (the example is used only when IKE is used for creating security association. For the encrypted map used by the security association set up through manual work, a given encrypted map contains only a transform set.).

crypto ipsec transform-set one

transform-type esp-des esp-sha-

hmac crypto ipsec transform-set two

transform-type ah-sha-hmac esp-des esp-sha-

hmac crypto map aaa 100 ipsec-isakmp

match address aaa

set transform-set one two

set peer 192..2.2.1

In this example, when the communication matches with access list aaa, the security association can use transform set one (first priority level) and set 2 (second priority level), which depends on the set and the matching with the transform set on the opposite terminal.

Relevant command

crypto map (global configuration)

crypto map (interface configuration)

crypto map local-address

match address

set peer

set pfs

set security-association lifetime

set security-association inbound

set security-association outbound

show crypto map

4.1.22 show crypto ipsec sa

The command “show crypto ipsec sa” can be used for checking the settings used by the current security association.

Syntas

show crypto ipsec sa [map *map-name* **|interface** *interface-id* **] [detail]**

Parameter

Parameter	Description
map m ap-name	(optional)showing the existing security association created by the encrypted map
interface *interface-id*	(optimal) Showing the existing security association created by the encrypted map on the identification interface.
Detail	(optimal) Showing the statistic information of security association.

Default

If no keyword is designated, all the security association will be shown.

Command mode

Supervisor mode

Explanation

none

Example

The following example is an output of the command “show crypto ipsec sa”

```
router#show crypto ipsec sa
detail Interface: Ethernet0/0
Crypto map name:aaa
local ident (addr/mask/prot/port): (191.1.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (197.7.7.0/255.255.255.0/0/0)
  local crypto endpt.: 192.2.2.87, remote crypto endpt.: 192.2.2.86
  inbound esp sas:
     spi:0x190(400)
        transform: esp-des esp-sha-hmac in
        use settings ={ Tunnel }
        no sa timing
```

```
        #pkts decaps: 0, #pkts decrypt: 0, #pkts auth: 0
        #pkts decaps err: 0, #pkts decrypt err: 0, #pkts auth err:
        0 #pkts replay failed: 0
    inbound ah sas:
      spi:0x12c(300)
        transform:    ah-md5-hmac
        in use settings ={ Tunnel }
        no sa timing
        #pkts decaps: 0, #pkts decrypt: 0, #pkts auth: 0
        #pkts decaps err: 0, #pkts decrypt err: 0, #pkts auth err:
        0 #pkts replay failed: 0
    outbound esp sas:
      spi:0x191(401)
        transform: esp-des esp-sha-hmac in
        use settings ={ Tunnel }
        no sa timing
        #pkts encaps: 0, #pkts encrypt: 0, #pkts auth: 0
        #pkts encaps err: 0, #pkts encrypt err: 0, #pkts auth err:
        0 #pkts replay failed: 0
    outbound ah sas:
      spi:0x12d(301)
        transform:    ah-md5-hmac
        in use settings ={ Tunnel }
        no sa timing
        #pkts encaps: 0, #pkts encrypt: 0, #pkts auth: 0
        #pkts encaps err: 0, #pkts encrypt err: 0, #pkts auth err:
        0 #pkts replay failed: 0
```

Relevant command

None

4.1.23 show crypto ipsec transform-set

The command “show crypto ipsec transform-set” can be used for checking all the configured transform set

Syntas

show crypto ipsec transform-set [*transform-set-name*]

Parameter

Parameter	Description
transform-set-name	(optional) Showing the transform set of the designated transform-set-name.

Default

If the keyword is not used, all the transform set will be shown on the router.

Command mode

Supervisor mode

Explanation

none

Example

The example below is an output of the command “show crypto ipsec transform-set”.

```
router# show crypto ipsec transform-
set Transform set aaa: { esp-des }
        will negotiate ={ Tunnel }
Transform set bbb: { ah-md5-hmac esp-3des
        } will negotiate ={ Tunnel }
```

Relevant command

None

4.1.24 show crypto map

The command “show crypto map” can be used for checking the configuration of the encrypted map.

Syntas

show crypto map [*map-name*]

Parameter

Parameter	Description
map-name	(optional) Showing the encrypted map designated by map-name.

Default

If no keyword is designated, all the encrypted map configurations will be shown on the router.

Command mode

Supervisor mode

Explanation

none

Example

The following example is an output of the command “show crypto map”.

```
router_config#show crypto map
Crypto Map aaa 100 ipsec-manual
        Extended IP access list aaa
  permit ip 192.2.2.0 255.255.255.0 193.3.3.0
        255.255.255.0 peer = 192.2.2.1
        Inbound esp spi: 300 ,
         cipher key: 1234567812345678
         , auth key ,
        Inbound ah spi: 301 ,
         key: 000102030405060708090a0b0c0d0e0f ,
        Outbound esp spi: 300 ,
         cipher key: 1234567812345678
         , auth key ,
        Outbound ah spi: 301 ,
         key: 00010203040506070809 0a0b0c0d0e0f
        Transform sets={ 1}
Crypto Map aaa 101 ipsec-isakmp
        Extended IP access list bbb
             permit ip 191.1.1.0 255.255.255.0 197.7.7.0
        255.255.255.0 peer = 192.2.2.19
        PFS (Y/N): N
        Security association lifetime: 2560 kilobytes/3600
        seconds Transform sets={ 1, 2,}
```

Relevant command

None

4.1.25 show crypto identification

To view the ID configuration, run **show crypto identification**.

show crypto identification

Parameter

None

Default

All ID configuration is displayed.

Command mode

EXEC

Explanation

None

Example

The following information appears after the **show crypto identification** command is run:

```
router_ config#show crypto identification
crypto identification default_local_identity
fqdn "inside"
crypto identification
  aa fqdn "outside"
```

Related command

None

4.1.26 transform-type

The command “transform-type” is used for setting transform type under configuration status of encryption transform.

Syntas

transform-type *transform1 [transform2[transform3]]*

Parameter

Parameter	Description
transform1	Less than 3 transforms can be designated. These transforms define IPSec

	transform2 security protocol and algorithm. The acceptable transform value will be *transform3* illustrated in “Direction for Use”.

Default

The default transform type is ESP-DES (ESP applies DES encryption algorithm)

Command mode

Configuration mode of Encryption Transform

Explanation

Transform set can designate one or two IPSec security protocol (or ESP, or AH or both two) and designate the algorithm used together with the selected security protocol. ESP and AH IPSec security protocol is detailed in the part “IPSecprotocol ： Encapsulation Security Protocol and Authentication Head”.

The definition of transform set can designate one to three transforms---each transform represents an IPSec security protocol (ESP or AH) and the mix of the algorithms to be used. When some transform set is used for IPSec security negotiation, the whole transform set (protocol, algorithm and the mix of other settings) shall match with a transform set of the opposite terminal.

In a transform set, AH protocol, ESP or both two can be designated. If an ESP is designated in transform set, only ESP encryption exchange can be defined, and both ESP encryption exchange and ESP verification transform can defined.

Choosing Transform for Transform Set: Workable Transform Mix					
Choose one from AH transform		Choose one from ESP encryption transform		Choose one from ESP verification transform	
Transform	Description	Transform	Description	Transform	Description
ah-md5-hmac	AH verification algorithm with MD5(HMAC variable)	esp-des	ESP Encryption Algorithm employing DES	esp-md5-hmac	ESP verification algorithm with MD5 (HMAC variable)
ah-sha-hmac	AH verification algorithm with SHA (HMAC variable)	esp-3des	Applying ESP encryption algorithm of 3DES	esp-sha-hmac	ESP verification algorithm with SHA (HMAC variable)

IPSecprotocol：ESP and AH

ESP and AH protocol provide security service for IPSec

ESP provides the services of subgroup encryption, the optional data verification and anti-replay.

AH provides the service of data verification and anti-replay.

ESP uses an ESP head and an ESP end to encapsulate the protected data or a complete IP self-search address data packet (or only the effective load). AH is inlaid into the protective data. It inserts an AH head directly into the back of outside IP head, inside IP data packet or the front of effective load. The whole IP data message should be encapsulated and protected in the tunnel mode, while in transport mode only the effective load in IP data message is encapsulated/protected. For further information of these two modes, please refer to the description of mode commands.

Choosing appropriate transform

IPSec transform is relatively complex. The following prompts can help you choose the right transform:

- If the data confidentiality is needed to provide, ESP encryption transform can be used.
- If the data verification of outside IP message head and data are needed to provide, AH transform can be used.
- If an ESP encryption transform is used, ESP verification transform or AH transform can be considered to be used for providing the verification service of transform set.
- If the function of data verification is needed (or ESP or AH is used), MD5 verification algorithm or SHA algorithm can be chosen. SHA algorithm is more vigorous than MD5 algorithm, but it takes more time.

Configuration status of encryption transform

After the command “crypto ipsec transform-set” is executed, the configuration status of encryption transform will be accessed. Under this state, the mode can be changed into tunnel mode or transport mode (it is optional change). After these changes are made, global configuration mode can be restored by typing in “exit”. For more information of these optional changes, please refer to the detailed illustration of mode commands.

Changing the existing transform

If one or multiple transforms are designated for a transform set in the command “transform-type”, these designated transforms will replace the existing transform of transform set. If the command “transform-type” is changed, the change will be applied to the encryption map referring to the transform set. But the change will not be applied to the existing security association and will be used for creating new security association. The command “clear crypto sa” can be used for deleting the partial or whole security association database.

Example

The example below defines a transform set

```
crypto ipsec transform-set one
transform-type esp-des esp-sha-hmac
```

Relevant command

crypto ipsec transform-set

mode

set transform-set

show crypto ipsec transform-set

Chapter 5 **IKE Protocol Commands**

This chapter discusses the commands for Internet Secret Key Exchange Security Protocol (IKE).

IKE is a kind of the standard of secret key management protocol and is used together with IPSec protocol.

IPSec is allowed not to use IKE. However, IKE advances the function of IPSec by offering extra functions, flexibility and the simplification of IPSec standard configuration.

IKE is a kind of mixed protocol, it realizes Oakley secret key exchange and Skeme Secret Key Exchange within the framework of Internet Security Association and Secret Key Management Protocol (（ISAKMP）(ISAKMP， Oakley and Skeme are the security protocol realized by IKE).

5.1 Internet Secret Key Exchange Security Protocol Command

5.1.1 authentication(IKE policy)

ISAKMP policy configuration command can be used for designating authentication method in IKE policy that defines a group of parameters used during IKE negotiation. The “no” format of the command can be used for restoring the default value of authentication method.

Syntas

authentication { pre-share|rsa-sig|rsa-encr}

no authentication { pre-share|rsa-sig|rsa-encr}

Parameter

Parameter	Description
pre-share	Designating pre-shared secret key as authentication method
rsa-sig	Designating RSA signature as authentication method
rsa-encr	Designating RAS real time encryption as authentication method

Default

Authentication method of pre-shared secret key

Command mode

Configuration mode of ISAKMP Policy

Explanation

The command is used for designating the authentication method in IKE policy

In order to designate pre -shared secret key, these pre- shared secret key shall be configured simultaneously. (Command “crypto isakmp key” is used)

Example

The pre-shared secret key is used as its authentication method for configuring IKE policy in this example.

```
router_config#crypto isakmp policy 10
router_config_isakmp# authentication pre-share
router_config_isakmp# exit
router_config #
```

Relevant command

crypto isakmp key

crypto isakmp policy

encryption(IKE policy)

group(IKE policy)

hash(IKE policy)

lifetime(IKE policy)

show crypto isakmp policy

5.1.2 clear crypto isakmp

The global configuration command “clear crypto isakmp” is used for clearing the running IKE linkage.

Syntas

clear crypto isakmp [**map** *map-name* | **peer** *ip-address*]

Parameter

Parameter	Description
map *map-name*	(optional) Clearing IKE linkage of encrypted map named map-name.
peer *ip-address*	(optional) Clearing *ip-address*IKE linkage of the opposite terminal.

Default

If the parameters of map and peer are not used, all the existing IKE linkage is cleared when the command is issued.

Command mode

Supervisor mode

Explanation

The command is used for clearing the active IKE linkage.

Example

This example clears isakmp linkage

```
Router# show crypto isakmp sa
     dst              src              state          state-id        conn
192.2.2.19       192.2.2.199     <I>M_SA_SETUP          1          aaa 100
Route# clear crypto isakmp
Router# exit
Router#show crypto isakmp sa
Router#
```

Relevant command

show crypto isakmp sa

5.1.3 crypto isakmp key

The global configuration command “crypto isakmp key” is used for configuring pre-shared authentication secret key. The secret key shall be configured for designating pre-shared secret key in IKE policy at any time. The “no” format of the command can be used for deleting pre-shared authentication secret key.

Syntas

crypto isakmp key *keystring peer-address*

no crypto isakmp key *keystring peer-address*

Parameter

Parameter	Description
keystring	Designating pre-shared secret key by using letter, number and character to form a random mix with 128 bytes at the most.
peer-address	Designating IP address of remote terminal

Default

Pre-shared authentication secret key without default

Command mode

global configuration mode

Explanation

If IKE policy includes pre-shared secret key that is used as authentication method, these pre-shared secret key shall be configured on the two terminals. Otherwise, the policy shall not be adopted (The policy will not be submitted in IKE process for configuration).

Example

Designating pre-shared secret key and designating remote terminal by using IP address.

crypto isakmp key abcdefghijkl 192.2.2.1

Relevant command

authentication (IKE policy)

5.1.4 crypto isakmp policy

The global configuration command “crypto isakmp policy” is used for defining IKE policy. IKE policy defines a set of parameters used during IKE negotiation. The “no” format of the command is used for deleting IKE policy.

Syntas

crypto isakmp policy *priority*

no crypto isakmp policy *priority*

Parameter

Parameter	Description
priority	Identifying the priority level of IKE policy by employing the integer from 1 to 10000. 1 represents top priority level and 10000 represents bottom priority level.

Default

There is a default policy. The policy is always on the bottom priority level. In this default policy, encryption, hash, authentication, Diffie-Hellman group and lifetime parameter are all set as default value.

If no value is designated for the specific parameter in creating an IKE policy, the default value will be applied to the parameter.

Command mode

global configuration mode

Explanation

The command is used for designating the parameter that is to be used during IKE negotiation (These parameters are used for creating IKE SA).

The command is used for accessing the configuration status of ISAKMP. Under the configuration status of ISAKMP policy, the following commands are effective in designating parameter value in the policy.

- encryption(IKE policy); default value =56 byte DES-CBC
- hash(IKE policy); default value =SHA-1
- authentication(IKE policy); default value =Pre-Shared Key
- group(IKE policy); default value =768 byte Diffie-Hellman
- lifetime(IKE policy); default value =86400 seconds.

If one of these commands are not designated for the policy, the default value of the parameter will be employed.

Multiple IKE policies can be configured to the two terminals of IPSec. When IKE negotiation starts in an attempt to find the common policy configured on the two terminals, it will set out from the policy of top priority level designated on the opposite terminal.

Example

The example below configures two ISAKMP policies

crypto isakmp policy 10

```
hash md5
authentication pre-
share group 2
lifetime 5000
crypto isakmp policy 20
authentication pre-
share lifetime 10000
```

The result of above configuration is the policy below:

```
Router# show crypto isakmp policy
Protection suite of priority 10
        encryption algorithm:    DES   - Data Encryption Standard (56 bit keys).
        hash algorithm:           Message Digest 5
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #1 (768 bit)
        lifetime:                5000 seconds
Protection suite of priority 20
        encryption algorithm:    DES   - Data Encryption Standard (56 bit keys).
        hash algorithm:           Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #1 (768 bit)
        lifetime:                10000 seconds
Default protection suite
        encryption algorithm:    DES   - Data Encryption Standard (56 bit keys).
        hash algorithm:           Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #1 (768 bit)
        lifetime:                86400 seconds
```

Relevant command

authentication(IKE policy)

encryption(IKE policy)

group(IKE policy)

hash(IKE policy)

lifetime(IKE policy)

show crypto isakmp policy

5.1.5 crypto isakmp keepalive

To configure IPSec dead peer detection (DPD), run **crypto isakmp keepalive** in global configuration mode. The command is used to promptly detect and clear the locally-stored information about the peer node when the peer node cannot be reached. To cancel IPSec DPD, run **no crypto isakmp keepalive**.

crypto isakmp keepalive *seconds types*

no crypto isakmp keepalive

Parameter

Parameter	Description
Seconds	Specifies the interval of PDP message forwarding. It ranges from 10 to 3600 seconds.
types	Specifies the conditions that trigger the DPD message transmission. The default condition is **on-demand**. <2-69>: retry times after the DPD detection failure On-demand: means that the DPD message is sent only when the message fails to be sent. Periodic: means the DPD message is sent when the path is free.

Default

The default value of the parameter **seconds** is 10.

The default value of the **types** parameter is **on-demand**.

The default retry times after the DPD detection fails is 5.

Command mode

Global configuration mode

Explanation

When the function is started, the peer must support DPD.

Example

The following example shows that a DPD whose interval is 10, whose failed resending times is 5 and whose type is **on-demand** is specified:

crypto isakmp keepalive 10 5

The following example shows that a DPD whose interval is 10, whose failed resending times is 5 and whose type is **periodic** is specified:

crypto isakmp keepalive 10 5 periodic

The following example shows that the DPD configuration is canceled:

no crypto isakmp keepalive

Related command

None

5.1.6 debug crypto isakmp

Examining the information of related message interactive processing in IKE negotiation.

Syntas

debug crypto isakmp

Parameter

None

Default

The related information is not shown under default status.

Command mode

Supervisor mode

Explanation

Some important information related to IKE negotiation is shown in the form below:

Showing Information	Connotation of Information
ISAKMP(xxx): no acceptable Oakley Transform ISAKMP(xxx) : negotiate error NO_PROPOSAL_CHOSEN	ISAKMP policies configured by two terminals are not matchable.(The opposite terminal starts negotiation)
ISAKMP(xxx): no acceptable Proposal in IPsec SA ISAKMP(xxx) : negotiate error NO_PROPOSAL_CHOSEN	IPSec policies configured by two terminals do not match. (The opposite terminal starts negotiation.)
ISAKMP(xxx): ISAKMP: not found matchable policy	IP Sec rules configured by two terminals do not match.
ISAKMP(xxx): dealing with Notify Payload ISAKMP: Notify-Message: NO_PROPOSAL_CHOSEN	ISAKMP policies configured by two terminals do not match. (The local terminal starts negotiation, in the first phase)

ISAKMP(xxx): dealing with Notify Payload ISAKMP: Notify-Message: NO_PROPOSAL_CHOSEN	IPSec strategies configured by two terminals do not match, or the configured rules do not match (access-list). (The local terminal starts negotiation, in the second phase.
ISAKMP(xxx): negotiate error ATTRIBUTES-NOT-SUPPORTED	The local terminal does not support the attribute suggested by the opposite terminal.
ISAKMP(xxx): dealing with Notify Payload ISAKMP:Notify-Message: ATTRIBUTES-NOT-SUPPORTED	The opposite terminal does not support the attribute suggested by the local terminal.

Relevant command

show crypto ipsec sa

show crypto isakmp sa

debug crypto packet

5.1.7 encryption(IKE policy)

The configuration command of ISAKMP policy “encryption(IKE policy)” is used for designating encryption algorithm in IKE policy. IKE policy defines a set of parameters that are used during IKE negotiation. The “no” format of the command can be used for restoring encryption algorithm as the default value.

Syntas

encryption {**des**|**3des**}

no encryption {**des**|**3des**}

Parameter

Parameter	Description
des	Designating DES as encryption algorithm
3des	Designating 3DES as encryption algorithm

Default

DES encryption algorithm

Command mode

Configuration mode of ISAKMP policy

Explanation

The command is used for designating encryption algorithm used in IKE policy

Example

This example configures encryption algorithm as DES encryption algorithm in IKE policy (All the other parameters are set as default value)

router_config# crypto isakmp policy 10

router_config_isakmp# encryption des

router_config_isakmp# exit

router_config#

Relevant command

authentication(IKE policy)

crypto isakmp policy

group(IKE policy)

hash(IKE policy)

lifetime(IKE policy)

show crypto isakmp policy

5.1.8 group(IKE policy)

The configuration command of ISAKMP strategy “group (IKE policy)” is used for designating Diffie-Hellman group in IKE policy. IKE policy defines a set of parameters that are used during IKE negotiation. The “no” format of the command can be used for restoring Diffie-Hellman group as default value.

Syntas

group {**1**|**2**} **no**

group {**1**|**2**}

Parameter

Parameter	Description
1	Designating 768 byte Diffie-Hellman group
2	Designating 1024 byte Diffie-Hellman group

Default

768 byte Diffie-Hellman group (group 1)

Command mode

Configuration mode of ISAKMP policy

Explanation

The command is used for designating Diffie-Hellman group used in IKE policy

Example

This example configure IKE policy as 1024 byte Diffie-Hellman group (all the other parameters are set as default value)

router_config# crypto isakmp policy 10
router_config _isakmp# group 2
router_config _isakmp# exit
router_config#

Relevant command

authentication(IKE policy)

crypto isakmp policyen

cryption(IKE policy)

hash(IKE policy)

lifetime(IKE policy)

show crypto isakmp policy

5.1.9 hash(IKE policy)

The configuration command of ISAKMP policy “hash(IKEpolicy)” is used for designating hash algorithm in IKE policy IKE policy defines a set of parameters that are used during IKE negotiation. The “no” format of the command can be used for restoring hash algorithm as default SHA-1 hash algorithm.

Syntas

hash {**sha**|**md5**}

no hash {**sha**|**md5**}

Parameter

Parameter	Description
sha	Designating SHA-1(HMAC variant) as hash algorithm.
md5	Designating MD5(HMAC variant)as hash algorithm

Default

SHA-1 hash algorithm

Command mode

Configuration Status of ISAKMP policy

Explanation

The command is used for designating hash algorithm used in IKE policy

Example

The Example configures IKE policy as using MD5 hash algorithm (all the other parameters are set as default value):

router_config # crypto isakmp policy

10 router_config _isakmp# hash md5

router_config _isakmp# exit

router_config#

Relevant command

authentication(IKE policy)

crypto isakmp policy encryption(IKE policy)

group(IKE policy)

lifetime(IKE policy)

show crypto isakmp policy

5.1.10 lifetime(IKE policy)

The configuration command of ISAKMP policy “lifetime(IKE policy)” is used for describing lifetime of IKE SA. The “no” format of the command can be used for restoring SA lifetime as default value.

Syntas

lifetime *seconds*

no lifetime *seconds*

Parameter

Parameter	Description
seconds	Designating the lasting seconds before IKE SA is disabled.

Default

86400 seconds

Command mode

Configuration mode of ISAKMP policy

Explanation

The command is used for designating the existing time of IKE SA before IKE SA is disabled.

When IKE starts negotiation, the agreement is reached first on the security parameters for its dialogue. These accordant parameters is referred by SA. IKE SA is reserved till the lifetime loses effect. Before IKE SA loses effect, it can be re-used by the consequent IKE negotiation, which can save time in setting new IPSec SA. New IKE SA is negotiated before IKE SA loses effect. In order to save the time of setting IPSec, the relative long IKE SA lifetime shall be set. The shorter the configured lifetime is, the more secure the IKE negotiation is.

Notes:

When the local terminal starts IKE negotiation with the opposite terminal, the policy can be chosen only on the condition that the lifetime of opposite terminal policy is shorter than or equals to that of local terminal policy.

If the lifetime is unequal,choose the shorter one.

Example

The Example configures the lifetime of security association of IKE policy as 600 seconds (all the other parameters are set as default value)

router_config# crypto isakmp policy 10

router_config_isakmp# lifetime 600

router_config_isakmp# exit

router_config#

Relevant command

authentication(IKE policy)

crypto isakmp policy

encryption(IKE policy)

group(IKE policy)

hash(IKE policy)

show crypto isakmp policy

5.1.11 show crypto isakmp policy

Syntas

show crypto isakmp policy

Parameter

None

Command mode

Supervisor mode

Explanation

The command “show crypto isakmp policy” is used for browsing each parameter of IKE policy.

Example

The following is the output of the command “show crypto isakmp policy” after two IKE policies are configured (priority level 10 and 20 separately)

```
router# show crypto isakmp policy
Protection suite of priority 10
        encryption algorithm:     DES    - Data Encryption Standard (56 bit keys).
        hash algorithm:             Message Digest 5
        authentication method:    Pre-Shared Key
        Diffie-Hellman group:     #1 (768 bit)
        lifetime:                   5000 seconds
Protection suite of priority 20
        encryption algorithm:     3DES - Triple Data Encryption Standard.
        hash algorithm:             Secure Hash Standard
```

```
        authentication method:    Pre-Shared Key
        Diffie-Hellman group:     #2 (1024 bit)
        lifetime:                 10000 seconds
    Default protection suite
        encryption algorithm:     DES  - Data Encryption Standard (56 bit keys).
        hash algorithm:           Secure Hash Standard
        authentication method:    Pre-Shared Key
        Diffie-Hellman group:     #1 (768 bit)
        lifetime:                 86400 seconds
```

Relevant command

authentication(IKE policy)

crypto isakmp policy

encryption(IKE policy)

group(IKE policy)

hash(IKE policy)

lifetime(IKE policy)

5.1.12 show crypto isakmp sa

The command “show crypto isakmp sa” is used for showing all the current IKE SA.

Syntas

show crypto isakmp sa

Parameter

none

Command mode

Supervisor mode

Explanation

The following is output example of the command “show crypto isakmp sa” after two terminal hosts have successfully accomplish IKE negotiation.

MyPeerRouter# show crypto isakmp sa

dst	src	state	state-id	conn
192.2.2.19	192.2.2.199	<I>Q_SA_SETUP	2	aaa 100

192.2.2.19 192.2.2.199 <I>M_SA_SETUP 1 aaa 100

The form below shows the possible different status in the output of the command “show crypto isakmp sa”. When ISAKMP SA exists, it is under quiet state in most time (Q_SA_SETUP)

The status in master model exchange	
Status	Explanation
M_NO_STATE	The phase is “initial stages” and no status exist.
M_SA_EXCH	The terminal has formed the parameter of ISAKMP SA.
M_KEY_EXCH	The terminal has exchanged common secret key of Diffie-Hellman and generated shared secret.ISAKMP SA is not authenticated.
M_SA_SETUP	ISAKMP SA has been authenticated. Quick model exchange starts

The Status in quick model exchange	
Status	Explanation
Q_IDLE_1	Quick model Status 1
Q_IDLE_2	Quick Model Status 2
Q_SA_SETUP	IPSec SA negotiation succeeds.

Relevant command

crypto isakmp policy

lifetime(IKE policy)