Security Configuration Command

Table of Contents

Chapter 1 AAA Authentication Configuration Commands

1.1 AAA Authentication Configuration Commands

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

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

AAA Authentication Configuration Commands include：

- aaa authentication enable default
- aaa authentication login
- aaa authentication password-prompt
- aaa authentication username-prompt
- aaa group server
- debug aaa authentication
- enable password
- server
- service_password-encryption
- username

1.1.1 aaa authentication enable default

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

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

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

parameter

parameter	description
method	At least one of the keywords described in Table 1.

default

If the default list is not set, only the enable password is checked. This has the same effect as the following command:

aaa authentication enable default enable

On the console, the enable password is used if it exists. If no password is set, the process will succeed anyway.

command mode

Global configuration

instruction

Use the aaa authentication enable default command to create a series of authentication methods that are used to determine whether a user can access the privileged command level. Method keywords are described in Table 1. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify none as the final method in the command line.

Table 0-1   aaa authentication enable default Methods

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

example

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

aaa authentication enable default line enable none

related commands

enable password

1.1.2   aaa authentication login

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

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

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

parameter

parameter	description
Default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods activated when a user logs in.
method	At least one of the keywords described in Table 2.

default

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

aaa authentication login default none

command mode

Global configuration

instruction

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

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

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

Table 0-2   AAA authentication login Methods

Keyword	Description
enable	Uses the enable password for authentication.
group	Uses the server group for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
group radius	Used RADIUS for authentication.

example

The following example creates an AAA authentication list called TEST. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+

returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

aaa authentication login TEST tacacs+ enable none

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

aaa authentication login default tacacs+ enable none

related commands

1.1.3   aaa authentication password-prompt

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

aaa authentication password-prompt *text-string*

no aaa authentication password-prompt *text-string*

parameter

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

default

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

command mode

Global configuration

instruction

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

Password:

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

example

The following example changes the text for the username prompt:

aaa authentication password-prompt YourPassword:

related commands

aaa authentication username-prompt

enable password

1.1.4   aaa authentication username-prompt

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

aaa authentication username-prompt text-string

no aaa authentication username-prompt text-string

parameter

parameter	description
text-string	String of text that will be displayed when the user is prompted to enter a username.

default

There is no user-defined text-string, and the username prompt appears as "Username."

command mode

Global configuration

instruction

Use the aaa authentication username-prompt command to change the default text that the software displays when prompting a user to enter a username. The no form of this command returns the username prompt to the default value:

Username:

Some protocols (for example, TACACS+) have the ability to override the use of local username prompt information. Using the aaa authentication username-prompt command will not change the username prompt text in these instances.

Note：

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

example

The following example changes the text for the username prompt:

aaa authentication username-prompt YourUsernam:

related commands

aaa authentication password-prompt

1.1.5 aaa group server

To group different RADIUS server hosts into distinct lists and distinct methods, enter the aaa group server radius command in global configuration mode. To remove a group server from the configuration list, enter the no form of this command.

aaa group server radius *group-name*

no aaa group server radius *group-name*

parameter

parameter	description
group-name	Character string used to name the group of servers.

default

No default behavior or values.

command mode

Global configuration

instruction

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

Example

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

aaa group server radius radius-group

related commands

server

1.1.6   debug aaa authentication

To display information on authentication, authorization, and accounting (AAA) TACACS+ authentication, use the debug aaa authentication command in privileged EXEC mode. To disable debugging output, use the no form of this command.

debug aaa authentication

no debug aaa authentication

parameter

default

disabled

command mode

EXEC

instruction

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

example

The following is sample output from the debug aaa authentication command.

```
switch#debug aaa authentication
AAA: Authen start (0x1f74208), user=, authen_type=ASCII, priv=0, method-list=default
AAA: Use authen method LOCAL (0x1f74208).
AAA: Authen CONT, need username.
AAA: Authen CONT, need password.
AAA: Authen ERROR (0x1f74208)! Use next method.
AAA: Authen FAIL(0x1f74208)! Method-list polling finish.
```

Output information	description
Authen start (0x1f74208), user=, authen_type=ASCII, priv=0, method-list=default	The authentication starts and the username is unknown. Uses ASCII-type authentication. The privileged level required for the user to enter is 0. Uses the default authentication method list. UserID ＝ 0x1f74208
Use authen method LOCAL (0x1f74208)	Uses local authentication method. UserID ＝ 0x1f74208
Authen CONT, need username	Prompts for username
Authen CONT, need password	Prompts for password
Authen ERROR (0x1f74208)! Use next	Indicates that the local authentication fails,

method	Uses the next method in the list.
Authen FAIL(0x1f74208)! Method-list polling finish	Method-list polling is finished. The authentication fails.

related commands

1.1.7 enable password

To set a local password to control access to various privilege levels, use the enable password command in global configuration mode. To remove the password requirement, use the no form of this command.

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

no enable password [level *number*]

parameter

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

default

No password is defined.

command mode

Global configuration

instruction

Can not have spaces in the password that the switch configures. When using the enable password command, you cannot input space if you enter a clear text password. The length of the clear text password cannot exceed 126 characters.

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

Our switch system only supports two types of encryption. The encryption type is 0 and 7 respectively. Parameter O indicates no password is defined and you enter a clear text password in the following encrypted-password blank. Parameter 7 indicates a

self-defined algorithm is used for encryption and you enter encrypted text password in the following encrypted-password blank. This encryted text password can be copied from the configuration file of other switch.

example

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

enable password 0 clever level 10

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

enable password 7 074A05190326

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

related commands

aaa authentication enable default

service password-encryption

1.1.8   server

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

server A.B.C.D

no server A.B.C.D

parameter

parameter	description
A.B.C.D	IP address of the server.

default

No server

command mode

Server-group configuration

instruction

You can add 20 different servers in a server group at most.

example

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

server 12.1.1.1

related commands

aaa group server

1.1.9   service password-encryption

To encrypt passwords, use the service password-encryption command in global configuration mode. To restore the default, use the no form of this command.

service password-encryption

no service password-encryption

parameter

default

No encryption

command mode

global configuration

instruction

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

example

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

switch_config#service password-encryption

related commands

username username password

enable password

password

1.1.10   username

To establish a username-based authentication system, use the username command in global configuration mode. Use the no form of this command to remove an established username-based authentication.

username *username* [**password** { *password* | [encryption-type] *encrypted-password* }] [**user-maxlinks** *number*] [**autocommand** *command*]

no username *username*

parameter

parameter	description
Username	Username character string
password	Password a user enters.
password	Clear text of the password character string
encryption-type	Encryption type
encrypted-password	Encrypted password a user enters.
user-maxlinks	Limits the user's number of inbound links.
number	Link number that established simultaneously.
autocommand	Causes the specified command to be issued automatically after the user logs in. The autocommand must be used in the end of the command line.
command	Executes automatically command character string

default

No username-based authentication system is established.

command mode

global configuration

instruction

The password is considered as empty character string when there is no password parameter. The trust-host will bind the user to the specified host. This user and other hosts cannot pass authentication when logging in switch. The user-maxlinks command limit the user's number of inbound links. User can use the show users command to check which kind of authentication that each online user passes.

White spaces are not allowed in the configured password of our switch. This also applies to the enable password command.

Our switch system only supports two types of encryption. The encryption type is 0 and 7 respectively. Parameter O indicates no password is defined and you enter a clear text password in the following encrypted-password blank. Parameter 7 indicates a

self-defined algorithm is used for encryption and you enter encrypted text password in the following encrypted-password blank. This encryted text password can be copied from the configuration file of other switch.

example

The following example adds a local user, its username is someone, its password is someother:

username someone password someother

The following example adds a local user, its user name is Oscar, its password is Joan, uses encryption-type 7, that is, the encrypted text password:

enable password 7 1105718265

Assuming the encrypted text password is 1105718265, which is obtained from the configuration file of other switch.

related commands

aaa authentication login

Chapter 2 RADIUS Configuration Commands

This chapter describes the commands used to configure RADIUS. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the implementation, RADIUS clients run on switches and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

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

1.2   RADIUS Configuration Commands

RADIUS Configuration Commands include：

- debug radius
- ip radius source-interface
- radius-server challenge-noecho
- radius-server deadtime
- radius-server host
- radius-server optional-passwords
- radius-server key
- radius-server retransmit
- radius-server timeout
- radius-server vsa send

1.2.1   debug radius

To display information associated with RADIUS, use the debug radius command in EXEC mode. To disable debugging output, use the no form of this command.

debug radius ｛*event | packet*｝

no debug radius ｛*event | packet*｝

parameter

parameter	description
event	Displays radius event
packet	Displays radius packet.

default

command mode

> EXEC

instruction

> Use this command to debug network system to locate the authentication failure reason.
>
> Switch#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	description
return message to aaa, Give me your username	It needs username
return message to aaa, Give me your password	It needs the password that corresponds to the username
inital transmit access-request [4] to 192.168.20.126 1812 <length=70>	Sends authentication request to RADIUS server for the first time. The server address is 192.168.20.126, port number 1812, packet length 70
retransmit access-request [4] to 192.168.20.126 1812 <length=70>	The server doesn't respond to the request in time. The authentication request will be retransmitted.
192.168.20.126 is dead to response [4]	The server doesn't respond after many times of retransmittion. This serve is marked as dead.
Have tried all servers，return error to aaa	RADIUS cannot complete this authentication and returns to error.

example

> The following example debugs RADIUS event:
>
> debug radius event

1.2.2 ip radius source-interface

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

no ip radius source-interface

parameter

parameter	description
interface-name	Name of the interface that RADIUS uses for all of its outgoing packets.

default

No default behavior or values

command mode

global configuration

instruction

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

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

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

example

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

ip radius source-interface vlan 1

related commands

ip tacacs source-interface

1.2.3　radius-server challenge-noecho

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

radius-server challenge-noecho

no radius-server challenge-noecho

parameter

default

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

command mode

global configuration

instruction

example

radius-server challenge-noecho

1.2.4 radius-server deadtime

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

radius-server deadtime minutes

no radius-server deadtime

parameter

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

default

Dead time is set to 0.

command mode

global configuration

instruction

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

example

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

radius-server deadtime 5

related commands

radius-server host

radius-server retransmit

radius-server timeout

1.2.5　radius-server host

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

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

no radius-server host ip-address

parameter

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

default

No RADIUS host is specified;

command mode

global configuration

instruction

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

example

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

radius-server host 1.1.1.1

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

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

related commands

aaa authentication

radius-server key

tacacs server

username

1.2.6 radius-server optional-passwords

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

radius-server optional-passwords

no radius-server optional-passwords

parameter

This command has no parameters or keywords.

default

disabled

command mode

global configuration

instruction

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

example

The following example configures the first login to not require RADIUS verification:

radius-server optional-passwords

related commands

radius-server host

1.2.7 radius-server key

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

radius-server key *string*

no radius-server key

parameter

parameter	description
string	Spedifies the encrypted key. This encrypted key must match the encrypted key that RADIUS server uses.

default

The encrypted key is the empty character string.

command mode

Global configuration

instruction

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

example

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

radius-server key firstime

related commands

radius-server host

tacacs server

username

1.2.8   radius-server retransmit

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

radius-server retransmit *retries*

no radius-server retransmit

parameter

parameter	description
retries	Maximum number of retransmission attempts. The default is 3 attempts.

default

    3 attemps

command mode

    global configuration

instruction

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

example

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

    radius-server retransmit 5

related commands

    radius-server timeout

1.2.9   radius-server timeout

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

    radius-server timeout *seconds*

    no radius-server timeout

parameter

parameter	description
seconds	Number that specifies the timeout interval, in seconds. The default is 5 seconds.

default

    5 seconds

command mode

    global configuration

instruction

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

example

Use this command to set the number of seconds a router waits for a server host to reply before timing out.

radius-server timeout 10

related commands

1.2.10 radius-server vsa send

To configure the network access server to recognize and use vendor-specific attributes, use the radius-server vsa send command. To restore the default, use the no form of this command.

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

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

parameter

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

default

disabled

command mode

global configuration

instruction

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

example

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

radius-server vsa send accounting

related commands

radius-server host

Chapter 3 Web Authentication Commands

1.3　Web Authentication Configuration Commands

- web-auth enable
- web-auth accounting
- web-auth authentication
- web-auth mode
- web-auth keep-alive
- web-auth holdtime
- web-auth authtime
- web-auth portal-server
- web-auth vlan-password
- web-auth kick-out
- show web-auth
- show web-auth interface
- show web-auth user
- debug web-auth event
- debug web-auth error
- debug web-auth verbose
- debug web-auth http event
- debug web-auth http request
- debug web-auth http
- debug web-auth

1.3.1　web-auth enable

description

web-auth enable

no web-auth enable

parameter

default

instruction

Use this command to enable web authentication feature on the routing interface, or packets are out of control of web authenticaiton.

Command mode

Interface configuration mode

example

The following command enables web authentication on interface vlan 5:

Switch_config_v5#web-auth enable

1.3.2   web-auth accounting

description

web-auth accounting *method-name*

no web-auth accounting

parameter

parameter	Description
method- name	The configured accounting method list in AAA.

default

disabled

instruction

The system uses the configured accounting method after user logging in. If the accounting operation fails, the user will be informed of the authentication failure. If not configured with any accounting method, the default method will be used.

command mode

interface configuraton mode

example

The following command configures an accounting method list named weba-acct and applies it to interface vlan 5:

Switch_config# aaa accounting network weba-acct start-stop radius
Switch_config_v5# web-auth account weba-acct

1.3.3   web-auth authentication

description

web-auth authentication *method-name*

no web-auth authentication

parameter

parameter	description
method- name	The configured authentication method list in aaa. The valid value range:N/A.

default

no authentication method

instruction

The system uses the configured authentication method after user logging in. If the authentication operation fails, the user will be informed of the authentication failure. If not configured with any accounting method, the default method will be used.

command mode

interface configuration mode

example

The following command configures an authentication method list named weba-acct and applies it to interface vlan 5:

Switch_config# aaa authentication login weba local
Switch_config_v5# web-auth authentication weba

1.3.4   web-auth mode

description

web-auth mode [*user* | *vlan-id*]

no web-auth mode

parameter

parameter	Description
user	Uses username and password to authenticate user. Valid value range：N/A。
vlan-id	Uses vlan id of the physical interface to authenticate user. Valid value range：N/A。

default

Use username and password to authentication user.

Instruction

User needs to fill in username and password information in web interface when using username and password for authentication. User only needs to click the login button in web interface when using vlan id for authentication.

command mode

interface configuration mode

example

The following example configures the authentication method of vlan interface 5 to vlan id method:

Switch_config_v5#web-auth mode vlan-id

1.3.5   web-auth keep-alive

description

web-auth keep-alive *keep-alive-time*

no web-auth keep-alive

parameter

parameter	Description
keep-alive-time	Period that user browser sends online notification in seconds. Valid value range is from 60 to 65535.

default

60 seconds

Instruction

After reconfiguring the keep alive, the user browser who has passed the authentication will send the online notification packet again according to the former period and then initiate using the new period. The user browser who   passes the authentication after configuring the keep alive will immediately implement the the configured period to send online notification packet.

command mode

EXEC

example

The following command configures the period that the user browser sends online notification packet to the switch to 180 seconds:

Switch_config#web-auth keep-alive 180

1.3.6   web-auth holdtime

description

web-auth holdtime *holdtime*

no web-auth holdtime

parameter

parameter	Description
holdtime	Holdtime that the switch tests whether a user is online. Valid value range is from 60 to 65535.

default

180 seconds

instruction

Switch checks whether a user is online by the online notification packet that the user browser sends, if no online notification packet is received during the holdtime, the switch will regard that the user has gone offline abnormally and then force the user to log out and stop accounting to this user.

command mode

EXEC

example

The following command configures holdtime to 600 seconds:

Switch_config#web-auth holdtime 600

1.3.7   web-auth authtime

description

web-auth authtime *authtime*

no web-authtime

parameter

parameter	Description
authtime	The maximum time from user being distributed DHCP address to user passing the authentication (including accounting). Valid value range is from 60 to 65535.

default

180 seconds

Instruction

The switch will assign a certain amount of resources for authentication after the user using the dhcp protocol. If the user failes to pass the authentication duringthe authtime, the switch will release the resources assigned to the user. If the user needs to launch the authentication again, then the dhcp needs to be reused to trigger the switch to assign a certain authentication resources for the user.

command mode

EXEC

example

The following command configures authtime to 360 seconds：

Switch_config#web-auth authtime 360

1.3.8　web-auth portal-server

description

web-auth portal-server *A.B.C.D*

no web-auth portal-server

parameter

parameter	Description
A.B.C.D	The actual destination that the user accesses to when using domain name for web access before passing the authentication. The valid value range: IP address of a certain layer 3 switch interface.

default

instruction

When a user is performing DNS analysis before passing the authentication, the ip address of the answer segment in the DNS reply packet will be modified to the address of the portal server. Then the http request of the user will be redistributed to the portal server. The inner porttal server of the switch will return to the corresponding web page accordong to the current configuration.

command mode

EXEC

example

The following example configures address of the portal server to 192.168.20.41:

Switch_config#web-auth portal-server 192.168.20.41

1.3.9 web-auth vlan-password

description

web-auth vlan-password *password*

no web-auth vlan-password

parameter

parameter	description
password	The user password when the vlan id is used for authentication. Valid value range:N/A.

default

instruction

When the vlan id is used for authentication, the switch uses 'vlan n'as the username, among which n is the corresponding vlan number. The password configured by this command will be used as the user password when the vlan id is used for authentication.

command mode

EXEC

example

The following command configures vlan-password to abc:

Switch_config#web-auth vlan-password abc

1.3.10 web-auth kick-out

description

web-auth kick-out *A.B.C.D*

parameter

parameter	Description
A.B.C.D	IP address of the user. Valid value range: N/A.

default

instruction

> This command deletes users with the given IP address from the switch. If the accounting has been charged against the user before deletion, the switch will stop accounting when deleting the user. After deletion, if user wants to pass the authentication again, user needs to use dhcp to distribute address to retrigger the authenticaion process.

Command mode

> Exec

example

> The following example deletes user at IP address 192.168.20.43:
>
> Switch_config#web-auth kick-out 192.168.20.43

1.3.11   show web-auth

description

> **show web-auth**

parameter

> none

default

> none

instruction

> This command is used to display the current web authentication configuration in the switch.

Command mode

> Priviledged mode

example

> The following example displays the current web authentication configuration in the switch:
>
> Switch_config#show web-auth
> web authentication parameters
> holdtime   3600
> authtime   600
> keep-alive   60
> portal-server   192.168.20.41

1.3.12 show web-auth interface

description

show web-auth interface [**vlan** | **superVlan** *intf-id]*

description

parameter	Description
intf-id	Routing interface number. Valid value range:N/A.

default

instruction

This command is used to display the web authentication configuration of the specified interface in the switch.

Command mode

priviledged mode

example

The following example displays the web authentication configuration on interface vlan1:

```
Switch_config#show web-auth interface Vlan 1
web authentication parameters
web-auth            enable
account-method      weba-acct
authen-method       weba
mode                 user
```

1.3.13 show web-auth user

description

show web-auth user

parameter

default

instruction

This command is used to display all users in the switch, including users that have passed the authentication and yet to pass the authentication.

Command mode

    Priviledged mode

example

    The following example displays the current users:

```
Switch#show web-auth user
IP               MAC-ADDR        state                  remain-time(seconds)
192.168.20.42    0008.74b7.3de1  WEBA_USER_AUTHENTICATED 3572
-------------------------------------
authenticated users: 1, authenticating users: 0
```

1.3.14   debug web-auth event

description

debug web-auth event

parameter

    none

default

    none

instruction

    This command is used to output event information during web authentication process, like receiving authentication request and so on.

Command mode

    priviledged mode

example

    Switch#debug web-auth event

1.3.15   debug web-auth error

description

    debug web-auth error

parameter

    none

default

    none

instruction

> This command is used to output all error information for error orientation.

Command mode

> Priviledged mode

Example

> Switch#debug web-auth error

1.3.16   debug web-auth verbose

description

> **debug web-auth verbose**

parameter

> none

default

> none

instruction

> This command makes the output informaiton of the command debug web-auth event become more detailed, including the user MAC address related to the event.

Command mode

> Priviledged mode

example

> Switch#debug web-auth verbose

1.3.17   debug web-auth http event

description

> **debug web-auth http event**

parameter

> none

default

> none

instruction

This command is used to output event information related to http in web authentication, like receiving socket connection request and so on.

Command mode

Priviledged mode

example

Switch#debug web-auth http event

1.3.18　debug web-auth http request

description

debug web-auth request

parameter

default

instruction

This command is used to output the content of http request.

Command mode

Priviledged mode

example

Switch#debug web-auth http request

1.3.19　debug web-auth http

description

debug web-auth http

parameter

default

instruction

This command is equal to perform the debug web-auth http event and the debug web-auth request command.

Command mode

Priviledged mode

example

Switch#debug web-auth http

1.3.20   debug web-auth

description

debug web-auth

parameter

default

instruction

This command is equal to enable all debugging switches of web authentication at the same time.

Command mode

Priviledged mode

example

Switch#debug web-auth