MAC Address Authentication Configuration

Contents

Chapter1 Mac Address Authentication Configuration

1.1 Mac Authentication Overview

MAC address authentication is based on the port and the mac address of the user access to network access control function modules.Initially, the switch mac address table does not exist the user's mac address table entries, the first user's message will reach the trigger switch mac address authentication, the authentication process does not require user participation (such as user name and password input related) , after the passage of the user authentication will be added to switch mac address mac address table after the user's traffic can be the mac address table entries directly from the content to be forwarded.

Authentication supports two authentication methods, the time domain in the configuration AAA configuration options:

Through the radius server for authentication;

By the local user database for authentication;

1.2 Mac Address Authentication Configuration

1.2.1 AAA-Related Configuration

MAC authentication which need to be configured to use AAA authentication for domain authentication.The radius server for authentication or choose the local user database authentication in the AAA authentication domain.

If not configured, use the default system configuration, certification domain.

When both are not configured, you can not be authenticated.

In the absence of user participation, mac address authentication in the authentication needs to construct associated user name and password, and now there are two methods:

a) mac address mode, in such a way, using the mac address as the user name and password authentication, fixed-length string of 12 characters, such as the mac address is 00:01:7a: 80:40:2b, the user name and password is "00017a80402b";

b) Fixed user name and password, in this way, the user configuration of fixed user name and password;

Default mode for the mac address.

When using a radius server for authentication, there are two authentication methods can be used for selection: 1) pap; 2) chap.

Radus default authentication mode for the pap.

AAA Authentication Domain, RADIUS server and the local user database configuration information 802.1x configuration related content.

The following only shows the Mac address authentication module to perform the command.

Table 1-1 Configure AAA Authentication Domain option

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Choice AAA Authentication Domain	**mac-authentication domain** *<name>*	Required
Configure user name format	**mac-authentication user-name-format {fixed account** *<name>* **password** *<psw>}* | **mac-address**	Optional
Configure radius authentication	**mac-authentication encryption {pap | chap}**	Optional

1.2.2 Enabling Configuration

Related parameters, it needs to start before they can be the mac address authentication.

Need to start the global mode and port mode mac authentication, the port of mac authentication before they can take effect.

Table 1-2 Enabling configuration

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Enable Global Configuration	**mac-authentication**	Required
Enter port configuration mode	**interface ethernet** *device / slot / port*	-
Enable the Port Configuration	**mac-authentication**	Required

1.2.3 Off Assembly Line Testing Configuration

As the mac does not use authentication protocol packets to interact, it can not take the initiative off the assembly line Operation, the system detects the user through the user packet flow off the assembly line judge.Mac authenticated users to go online, then start off the assembly line detection timer when the timer reaches the user traffic after the detection if detected in time to reach another off the assembly line did not detect the user traffic, then determine the user offline .

Table 1-3 Configuration off the assembly line testing

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Offline detect timer	**mac-authentication timer offline-detect** *<offline-time>*	Optional

configuration		

1.2.4 Silent Timer Configuration

Mac user authentication into a quiet state after the failure, in this state, the user can not continue with mac certified, so you can prevent users of the system impact.In the silent state, silent timer will start, when the regular time arrives, the user data is deleted, the user can continue to mac authentication.

Table 1-4 Silent Timer Configuration

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Offline detect timer configuration	**mac-authentication timer quiet** <*quiet-time*>	Optional

1.2.5 Mac-vlan Configuration Functions

Open this feature, user authentication is successful, the server will return the user vlan number, the system for dynamic hardware mac-vlan entries are configured, and dynamically create the vlan, and the user is adding the vlan port, so you can vlan access the network.

If the system has been configured with the mac address table static mac-vlan entry, the entry dynamic mac-vlan configuration fails, the user into a quiet state, can not access the network.

Create vlan dynamic, the system will automatically configure the uplink ports to join the vlan, and is configured to tag attributes.Default to GE port as an uplink port.

Table 1-5 Configure mac-vlan function

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Function on mac-vlan	**mac-authentication mac-vlan**	Optional
Enter port configuration mode	**interface ethernet** *device / slot / port*	-
Configure the port as uplink ports	**mac-authentication up-link**	Optional

1.2.6 Guest-Vlan Configuration Functions

User authentication into a quiet state after failure, can not access the network, if time allows users to access a particular vlan, you can open the guest vlan function.In turn, the user authentication into a quiet state after the failure is not, and go online, but users of the vlan for the guest vlan.

In the guest vlan user's online status, you start re-authentication timer, time will reach the re-certification, if certification is successful, exit the guest vlan online, and to the normal online status.

Table 1-6 Configuration features guest-vlan

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Enter port configuration mode	**interface ethernet** *device / slot / port*	-
Open port guest-vlan function	**mac-authentication *guest-vlan* <vid>**	Optional
Guest-vlan configuration re-authentication timer	**mac-authentication timer guest-vlan-reauth** *<time>*	Optional

1.2.7 Configuring User Features

Mainly provides the following features:

limit the number of users

Limit the number of users allowed on a port:

user authentication rate limits

To prevent the user authentication result in excessive cpu is under attack, the need for port user authentication rate limits.When the user authentication packet rate exceeds this limit, the port stops receiving authentication messages function, this time limit timeout timer starts when the timer reaches the time to restore this port after receiving the message authentication function.

Table 1-7 User Feature Configuration

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Enter port configuration mode	**interface ethernet** *device / slot / port*	-
The number of users allowed on the port	**mac-authentication max-users** *<number>*	Optional