

802.1x Configuration

Официальный дистрибьютор в России и СНГ ООО «ТМС»
Адрес: Россия, 117519, г. Москва, Варшавское ш., дом 133, помещение 370

Тел: +7 (495) 723-81-21
Факс: +7 (495) 723-81-22
Техподдержка 24/7: +7 (495) 723-33-33
E-mail: sales@tmc.ru
Сайт: www.dgsys.ru

Table of Contents

Chapter 1 802.1x Configuration.....	1
1.1 802.1x Configuration Task List.....	1
1.2 802.1x Configuration Tasks.....	1
1.2.1 Configuring 802.1x Authentication on the Port.....	1
1.2.2 Configuring 802.1x on Multiple Ports Authentication.....	2
1.2.3 Configuring 802.1x Re-Authentication.....	3
1.2.4 Configuring 802.1x Authentication Retry Times.....	3
1.2.5 Configuring 802.1x Transmission Frequency.....	3
1.2.6 Configuring 802.1x User Binding.....	3
1.2.7 Configuring the Authentication Method on the 802.1x Port.....	4
1.2.8 Selecting the Authentication type for the 802.1x Port.....	4
1.2.9 Configuring MAB Authentication on the Port.....	4
1.2.10 Configuring 802.1x Accounting.....	5
1.2.11 Configuring 802.1x guest-vlan.....	5
1.2.12 Forbidding the Multi-NIC Supplicant.....	6
1.2.13 Resuming the Default Settings of 802.1x.....	6
1.2.14 Monitoring the 802.1x Authentication Configuration and State.....	6
1.3 802.1x Configuration Example.....	6

Chapter 1 802.1x Configuration

1.1 802.1x Configuration Task List

- Configuring 802.1x Authentication on the Port
- Configuring 802.1x on Multiple Ports of the Host
- Configuring 802.1x Re-Authentication
- Configuring 802.1x Authentication Retry Times
- Configuring 802.1x transmission frequency
- Configuring 802.1x User Binding
- Configuring the Authentication Method on the 802.1x Port
- Selecting the Authentication Mode for the 802.1x Port
- Configuring MAB Authentication on the Port
- Configuring 802.1x Accounting
- Configuring 802.1x guest-vlan
- Forbidding the Multi-NIC Supplicant
- Resuming the Default Settings of 802.1x
- Monitoring the 802.1x Authentication Configuration and State

1.2 802.1x Configuration Tasks

1.2.1 Configuring 802.1x Authentication on the Port

802.1x has three modes to control the port: force-authorized, force-unauthorized and enable.

Force-authorized means that the port has been authenticated and thus no authentication process is needed. In this mode, all users can conduct the data access control through the port. This mode is the default mode of the port. Force-unauthorized means that port authentication is not passed no matter what kind of authentication method you apply. In this mode, all users cannot conduct the data access control through the port.

Enable means that the 802.1x authentication protocol will be run on the port and the users who access the port will be authenticated by 802.1x. The successfully-authenticated users can conduct the data access control through the port. After enabling 802.1x authentication, you have to configure AAA authentication method.

Before the 802.1x is configured, you have to enable the 802.1x function by running the following commands:

Command	Purpose
dot1x enable	Enables the 802.1x function.

Run the following commands to enable the 802.1x authentication:

Command	Purpose
dot1x port-control auto	Sets the port to the 802.1x control mode.
aaa authentication dot1x {default list name} method	Configures 802.1x AAA authentication.

Run one of the following commands in interface configuration mode to select the 802.1x control mode:

Command	Purpose
dot1x port-control auto	Sets the port to the 802.1x control mode.
dot1x port-control force-authorized	The port authentication is authorized mandatorily.
dot1x port-control force-unauthorized	The port authentication is unauthorized mandatorily.
dot1x port-control misc-mab	The hybrid mode of multi-user and mab authentication

1.2.2 Configuring 802.1x on Multiple Ports Authentication

The 802.1x authentication is mainly for the single host user. At this time, the switch allows only one user to conduct the authentication and the access control. However, sometimes the port may connect multiple hosts through 802.1x-unsupported switching device, such as switch 1108. In order to make these hosts' users access successfully, you can enable the multi-host port access function. Actually, the authentication port may connect with multiple users. To ensure all users can be authenticated and visited, enable multiuser authentication function.

There are two kinds of multi-host authentication: one is the multiple-hosts mode and the other is multiple-auth mode. The multiple-hosts mode is that when one of the hosts passes through the authentication the port will be up and the other hosts (including the previous ones and the following ones) will not need authentication; the multiple-auth mode is that the switch authenticates each host respectively and these authentications do not interfere with each other. When only one user passes its authentication, the interface will be up; only when all users fail in their authentication, in another word, only when no successfully authenticated user exist on the interface, the interface will be down. This mechanism gives guarantee to respective authentication for each user and if a user fails in its authentication, other users still have the normal access rights.

Note: The multi-auth mode cannot coexist with guest vlan or mab. If an interface is in multi-auth mode, all users on the interface will be authenticated again.

Run the following command in interface configuration mode to activate the 802.1x multi-host port authentication:

Command	Purpose
dot1x authentication multiple-hosts	Sets 802.1x multiple-hosts interface access mode. As long as one user passes the

	authentication, the interface is up.
dot1x authentication multiple-auth	Sets 802.1x multiple-hosts interface authentication mode. The authentication for each user is in parallel.

1.2.3 Configuring 802.1x Re-Authentication

After the authentication is passed, the authentication to the client will still be conducted every interval to ensure the legality of the client's authentication.

In this case, you need to enable the re-authentication function. After the re-authentication is started, the authentication request will be periodically sent to the host.

Run the following commands to configure the re-authentication function.

Command	Purpose
dot1x re-authentication	Enables the re-authentication function.
dot1x timeout re-authperiod time	Configures the period of the re-authentication function.

1.2.4 Configuring 802.1x Authentication Retry Times

After the authentication is failed, the switch will continue forward request/ID packet to resume the authentication. If the device has no response when the authentication exceeds the max retry times, the authentication will be suspended.

Run the following commands to configure the max re-authentication times:

Command	Purpose
dot1x reauth-max time	Configures the retry times after the re-authentication function fails.

1.2.5 Configuring 802.1x Transmission Frequency

During 802.1x authentication, the packets will be transmitted to the client's host. You can adjust the data transmission to ensure the response of the client's host by controlling the 802.1x transmission frequency.

Run the following command to configure the transmission frequency.

Command	Purpose
dot1x timeout tx-period time	Sets the transmission frequency of the 802.1x packet.

1.2.6 Configuring 802.1x User Binding

You can bind the user to a certain port during 802.1x authentication to ensure the security of the interface access. To enable the 802.1x user binding, run the following command in interface configuration mode:

Command	Purpose
---------	---------

dot1x user-permit xxxz	Configures the user which is bound to the interface.
-------------------------------	--

1.2.7 Configuring the Authentication Method on the 802.1x Port

Different ports will be applied with different authentication methods during 802.1x authentication. By default, the 802.1x authentication adopts the default method.

To configure the 802.1x authentication method, run the following command in interface configuration mode:

Command	Purpose
dot1x authentication method yyy	Configures the 802.1x authentication method.

1.2.8 Selecting the Authentication type for the 802.1x Port

The authentication mode can be selected during the 802.1x authentication. The authentication class decides whether AAA uses the CHAP authentication or the EAP authentication. If the CHAP authentication is used, the challenge required by MD5 is locally generated; if the EAP authentication is used, the challenge is generated on the authentication server. Only one authentication mode can be applied to one interface. By default, the authentication mode is applied in global mode. When an authentication mode is configured for an interface, the authentication mode will be always used on the interface unless the negative form of the command is run to resume the default settings.

EAP-TLS adopts the electronic certificate as the evidence of authentication and follows the handshake regulations in TLS so that it is more secure.

Run the following command in global configuration mode to configure an authentication mode:

Command	Purpose
dot1x authen-type {chap eap}	Selects CHAP or EAP.

To configure the authentication mode, you also can run the following command in interface configuration mode:

Command	Purpose
dot1x authentication type {chap eap}	Selects CHAP or EAP, or just uses the configuration class in global mode.

1.2.9 Configuring MAB Authentication on the Port

When a peer device cannot run the 802.1x client software, the switch will adopt the MAB authentication mode and then the MAC address of the peer device will be sent as both the username and password to the radius server for authentication.

Note: You can run the **dot1x mabformat** command on a switch to specify the accounting ID and the password's format so that you make it sure that they are same with those on the radius server.

When the MAB authentication is enabled and the peer device, however, neither sends the eapol_start packet nor responds to the request_identity packet and

exceeds the timeout threshold, the switch regards this case as the evidence of not support the 802.1x authentication client on the peer device and then turns to the MAB authentication. When the switch sends the gained MAC address as the username and password to the Radius server for authentication, the authentication will still not succeed until the Radius server has authorized this MAC address.

Note: The MAB authentication mode cannot coexist with the multi-auth mode.

To enable the MAB authentication, you also can run the following command in interface configuration mode:

Command	Purpose
dot1x mab	Enables the MAB authentication on a port.

To set the format of the MAC address, you can run the following command in global configuration mode:

Command	Purpose
dot1x mabformat {1 2 3 4 5 6}	Chooses one MAC address' format from format 1 to format 6. The default format is 1.

1.2.10 Configuring 802.1x Accounting

The time the dot1x authentication is adopted you can conduct accounting. The actual accounting mechanism is that after dot1x authentication a judgment will be made as of whether the accounting is enabled on an authentication interface; if it is yes, the AAA interface will send the accounting request, and after receiving the request response information from the AAA module the authentication interface can allow the packets to pass through.

For the detailed accounting methods, refer to the relevant contents in the document AAA Settings.

For the correctness of the accounting data, the dot1x, after the accounting starts, will periodically use the AAA interface to send the update data to the server, while the AAA module, according to different AAA settings, decides whether to really send the accounting data.

Meanwhile, the dot1x re-authentication shall be enabled so that the switch will know a trouble as soon as it occurs on the supplicant.

To enable dot1x accounting and then set the accounting method, run the following commands in interface configuration mode:

Command	Purpose
dot1x accounting enable	Opens 802.1x accounting.
dot1x accounting method {method name}	Sets the accounting method.

1.2.11 Configuring 802.1x guest-vlan

Guest-vlan is to attribute the corresponding port with a limited access permission when the client does not respond. Guest-VLAN can be any configured VLAN in a system; when the configured guest -VLAN cannot reach the requirements, the port cannot enter the guest VLAN.

Note: If the authentication fails, the port will obtain no access permission.

To enable the guest vlan in global mode, run the following command:

Command	Purpose
dot1x guest-vlan	Opens the guest-VLAN on all ports.

At the initial time when the guest-vlan ID of each port is 0, the guest-vlan takes no effect even if it is enabled in global mode; only when the guest vlan ID is set in port configuration mode can the guest VLAN work.

Run the following command to set guest-vlan ID in port configuration mode:

Command	Purpose
dot1x guest-vlan {id(1-4094)}	Sets the VLAN ID of the guest VLAN on a port.

1.2.12 Forbidding the Multi-NIC Supplicant

This command can be used to forbid the supplicant terminal with multiple network adapters, preventing an agent from being occurred. Run the following command in port configuration mode:

Command	Purpose
dot1x forbid multi-network-adapter	Forbids the supplicant with multiple NICs.

1.2.13 Resuming the Default Settings of 802.1x

This command is used to resume all global configurations to the default settings. To configure the authentication mode, you also can run the following command in interface configuration mode:

Command	Purpose
dot1x default	This command is used to resume all global configurations to the default settings.

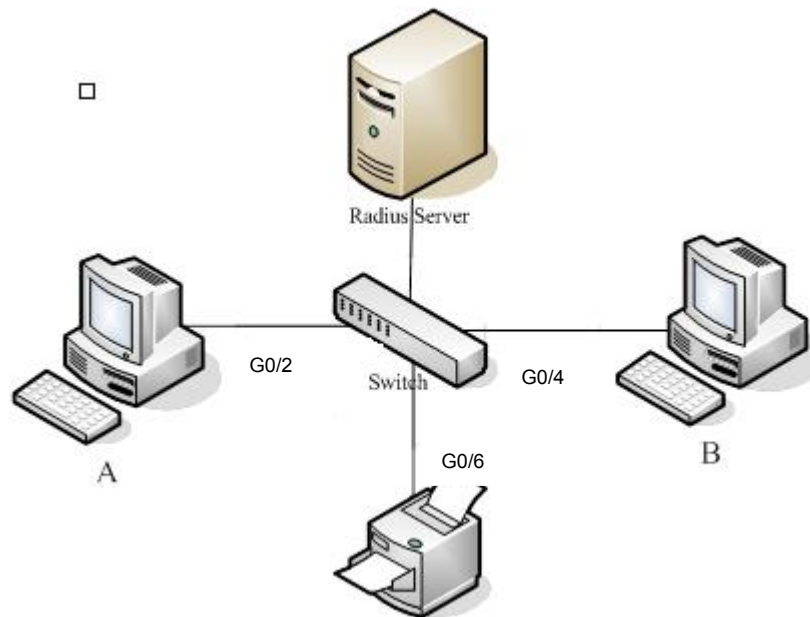
1.2.14 Monitoring the 802.1x Authentication Configuration and State

To monitor the 802.1x authentication configuration and state, run the following commands in EXEC mode:

Command	Purpose
show dot1x { interface statistics misc-mab-db }	Monitoring the 802.1x Authentication Configuration and State

1.3 802.1x Configuration Example

See the following figure:



Host A connects the G0/2 interface of the switch, host B the G0/4 interface, and host C the G0/6 interface; the radius-server host's IP is 192.168.20.2 and its key is TST; on the G0/2 interface the remote radius authentication, user-bind, accounting and re-authentication will be enabled altogether, on the G0/4 interface the local authentication, eap, multi-hosts and guest-vlan are enabled altogether, and on the G0/6 interface the MAB authentication is used and its MAC address' format is AA:BB:CC:DD:EE:FF.

Global configuration

```

username switch password 0 TST
username TST password 0 TST
aaa authentication dot1x TST-G0/2 group radius
aaa authentication dot1x TST-G0/4 local
aaa authentication dot1x TST-G0/6 group radius
aaa accounting network dot1x_acc start-stop group radius
dot1x enable
dot1x re-authentication
dot1x timeout re-authperiod 10
dot1x mabformat 2
dot1x guest-vlan
interface VLAN1
ip address 192.168.20.24 255.255.255.0
!
vlan 1-2
radius-server host 192.168.20.2 auth-port 1812 acct-port 1813
radius-server key TST
  
```

Configuration of interface f0/2

```

interface GigaEthernet0/2
dot1x port-control auto
dot1x authentication method TST-G0/2
  
```

```
dot1x user-permit radius-TST
dot1x accounting enable
dot1x accounting method dot1x_acc
```

Configuration of interface f0/4

```
Interface GigaEthernet0/4
dot1x authentication multiple-hosts
dot1x port-control auto
dot1x authentication method TST-G0/4
dot1x guest-vlan 2
```

Configuration of interface f0/6

```
interface GigaEthernet0/6
dot1x mab
dot1x authentication method TST-G0/6
```