802.1x Configuration

Model: S5900-24S4T2Q

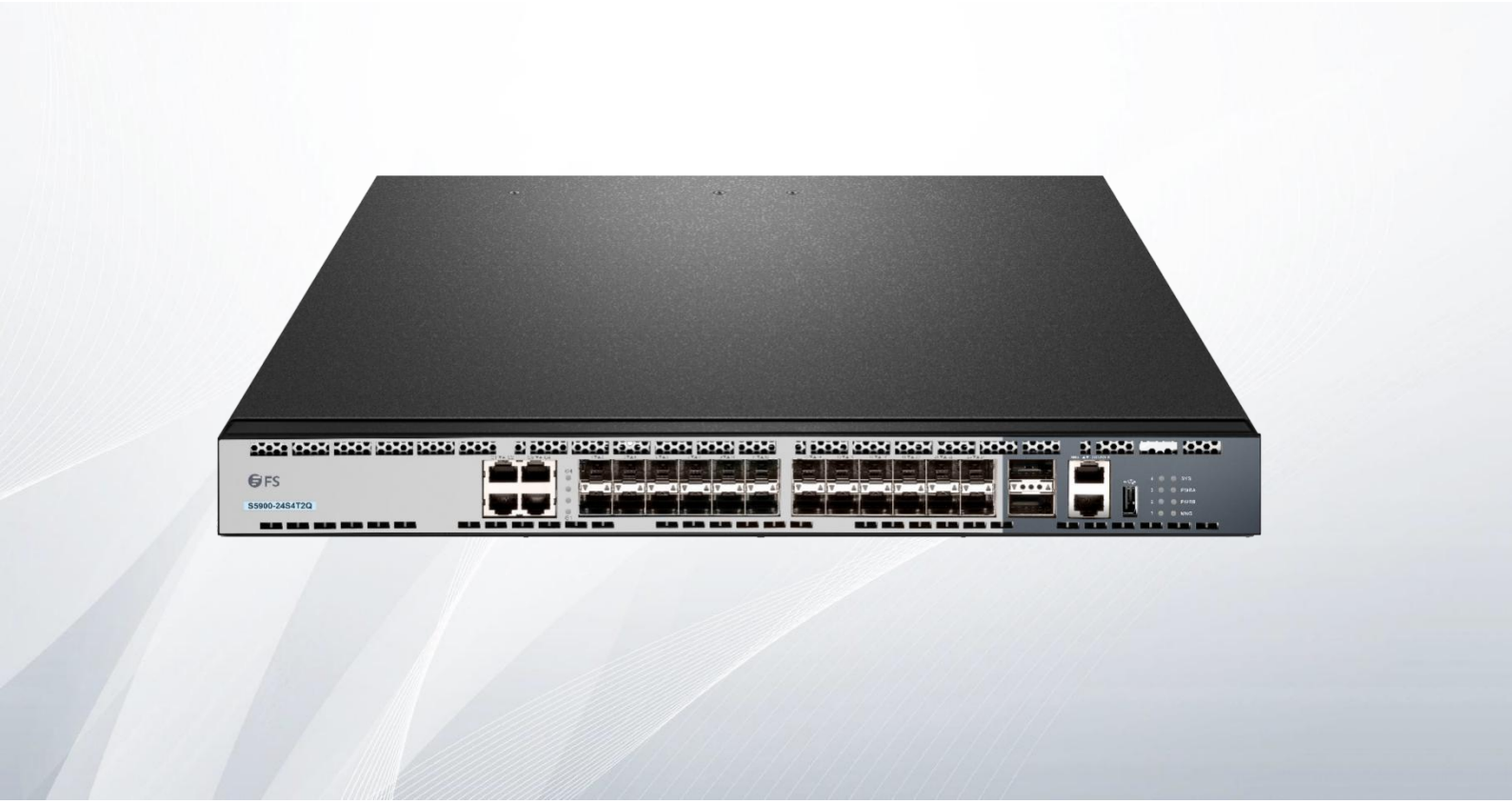

Table of Contents

1. Configuring 802.1x

1.1 802.1x Configuration Task List

- Configuring 802.1x port authentication
- Configuring 802.1x multiple port authentication
- Configuring maximum times for 802.1x ID authentication
- Configuring 802.1x re-authentication
- Configuring 802.1x transmission frequency
- Configuring 802.1x user binding
- Configuring authentication method for 802.1x port
- Selecting authentication type for 802.1x port
- Configuring 802.1x accounting
- Configuring guest-vlan
- Forbidding supplicant with multiple network cards
- Resuming default 802.1x configuration
- Monitoring 802.1x authentication configuration and state

1.2 802.1x Configuration Task

1.2.1 Configuring 802.1x Port Authentication

802.1x defines three control methods for the port: mandatory authentication approval, mandatory authentication disapproval and 802.1x authentication startup.

Mandatory authentication approval means the port has already passed authentication. The port does not need any authentication any more, and all users can perform dara access control through the port. The authentication method is defaulted by the port. Mandatory authentication disapproval means the port authentication does not get passed no matter what kind of method is applied. No user can perform the data access control through the port.

802.1x authentication startup means the port is to run 802.1x authentication protocol. 802.1x authentication will be applied to users who access the port. Only users who pass the authentication can perform data access control through the port. After the 802.1x authentication is started up, the AAA authentication method must be configured.

Run the following command to enable the 802.1x function before configuring 802.1x:

Run...	To...
dot1x enable	Enable the 802.1x function.

Run the following command to start up the 802.1x authentication:

Run...	To...
dot1x port-control auto	Configure the 802.1x protocol control method on the port.
aaa authentication dot1x {default |list name} method	Configure the AAA authentication of 802.1x.

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

Run...	To...
dot1x port-control auto	Start up the 802.1x authentication method on the port.
dot1x port-control force-authorized	Approve the mandatory port authentication.
dot1x port-control force-unauthorized	Disapprove the mandatory port authentication.

1.2.2 Configuring 802.1x Multiple Port Authentication

802.1x authentication is for the authentication of single host user. In this case, the switch allows only one user to perform authentication and access control. Other users cannot be authenticated and access unless the previous user exits authentication and access. In the case the port connects multiple hosts through switch devices, such as 1108 switch, that do not support 802.1x, you can start up the multiple port access function to make sure that all host users can access.

After a port is configured to multiple host authentication of 802.1x, the switch authenticates different host users. When authentication is approved, the host will be allowed to access through the switch (the MAC address of host is used for control). Theoretically, 802.1x cannot limit the number of host users. Because the switch controls the user authentication through the MAC address of user, the number of host users will be limited by the size of the MAC address table of the switch.

Run the following command in interface configuration mode to activate 802.1x multiple host authentication:

Run...	To...
dot1x multiple-hosts	Set the 802.1x multiple port authentication.

1.2.3 Configuring Maximum Times for 802.1x ID Authentication

When 802.1x authentication starts or 802.1x authentication is being performed again, 802.1x sends ID authentication request to guest hosts. If the request message is dropped or delayed because network problems, the requirement message will be sent again. If the message is resent certain times, 802.1x stops to send the message and the ID authentication fails.

You can reset the maximum times of ID authentication request according to different network conditions, ensuring the clients are authenticated successfully by the authentication server.

Run the following command in interface configuration command to set the maximum times for ID authentication request:

Run...	To...
dot1x max-req count	Set the maximum times for ID authentication request.

1.2.4 Configuring 802.1x Re-authentication

After first authentication is approved, the client will be authenticated every certain time to ensure the legality of the client. In this case, the re-authentication function needs to be enabled.

After the re-authentication function is enabled, 802.1x will periodically send the authentication request to the host.

You can run the following commands to configure the re-authentication function.

Run...	To...
dot1x re-authentication	Enable the re-authentication function.
dot1x timeout re-authperiod time	Configure the period of re-authentication.
dot1x reauth-max time	Configurethe retry times after the re-authentication fails.

1.2.5 Configuring 802.1x Transmission Frequency

In the process of 802.1x authentication, data texts will be sent to the host. The data transmission can be adjusted by controlling 802.1x transmission frequency so that the host response is successful.

Run the following command to configure the transmission frequency:

Run...	To...
dot1x timeout tx-period time	Set the message transmission frequency of 802.1x.

1.2.6 Configuring 802.1x User Binding

When 802.1x authentication is performed, you can bind a user to a certain port to ensure the security of port access. Run the following command in interface configuration mode to start up 802.1x user binding.

Run...	To...
dot1x user-permit xxxz	Configure a user that is bound to a port.

1.2.7 Configuring Authentication Method for 802.1x Port

The 802.1x authentication can be performed in different methods at different ports. In the default configuration, the 802.1x authentication adopts the default method.

Run the following command in interface configuration mode to configure the method of the 802.1x authentication:

Run...	To...
dot1x authentication method yyy	Configure the method of the 802.1x authentication.

1.2.8 Selecting Authentication Type for 802.1x Port

You can select the type for the 802.1x authentication. The 802.1x authentication type determines whether AAA uses Chap authentication or Eap authentication. Eap authentication supports the md5-challenge mode and the eap-tls mode. Challenge required by MD5 is generated locally when the Chap authentication is adopted, while challenge is generated at the authentication server when the eap authentication is adopted. Each port adopts only one authentication type. The authentication type of global configuration is adopted by default. Once a port is set to an authentication type, the port will use the authentication type unless you run the No command to resume the default value.

Eap-tls takes the electronic certificate as the authentication warrant and complies with the handshake rules in Translation Layer Security (tls). Therefore, high security is guaranteed.

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

Run...	To...
dot1x authen-type {chap|eap}	Select chap or eap.

Also run the following command in interface configuration mode:

Run...	To...
dot1x authentication type {chap|eap}	Select chap or eap or the configured authentication type in global mode.

1.2.9 Configuring 802.1x Accounting

The 802.1x authentication and 802.1x accounting can be performed at the same time. Its working mechanism is: after the dot1x authentication is approved, judge whether the accounting function is enabled on the authentication interface; if the accounting function is enabled, send the accounting request through the AAA interface; when the AAA module returns successful request

response message, the AAA interface can forward texts.

The accounting can adopt various accounting methods configured in the AAA module. For details, refer to AAA configuration.

After the beginning of accounting, dot1x periodically sends update message to the server through the AAA interface for obtaining correct accounting information. According to different AAA configuration, the AAA module decides whether to send the update message.

At the same time, You are required to enable the dot1x re-authentication function so that the switch can know when supplicant is abnormal.

Run the following commands in interface configuration mode to enable the dot1x accounting and to configure the accounting method:

Run...	To...
dot1x accounting enable	Enable the dot1x accounting.
dot1x accounting method {method name}	Configure the accounting method. Its default value is default.

1.2.10 Configuring 802.1x Guest-vlan

Guest-vlan gives relevant ports some access rights (such as downloading client software) when the client does not respond. Guest-vlan can be any configured vlan in the system. If the configured guest-vlan does not meet the conditions, ports cannot run in the guest-vlan.

Note:
There is no access right if the authentication fails.

Run the following command in the global mode to enable the guest-vlan:

Run...	To...
Dot1x guest-vlan	Enable the guest-vlan at all ports.

When the original value of guest-vlan id at each port is 0, guest-vlan cannot function even if guest-vlan is enabled in global mode. Only when guest-vlan id is configured in port configuration mode, guest-vlan can function.

Run the following command in port configuration mode to configure guest-vlan id:

Run...	To...
Dot1x guest-vlan {id (1-4094)}	Enable guest-vlan at all ports.

1.2.11 Forbidding Supplicant with Multiple Network Cards

Forbid the Supplicant with multiple network adapters to prevent agents. Run the following command in port configuration mode:

Run...	To...
dot1x forbid multi-network-adapter	Forbid the Supplicant with multiple network adapters.

1.2.12 Resuming Default 802.1x Configuration

Run the following command to resume all global configuration to default configuration:

Run...	To...
dot1x default	Resume all global configuration to default configuration.

1.2.13 Monitoring 802.1x Authentication Configuration and State

To monitor the configuration and state of 802.1x Authentication and decide which 802.1x parameter needs to be adjusted, run the following command in management mode:

Run...	To...
show dot1x {interface ....}	Monitor the configuration and state of 802.1x authentication.

1.3 802.1x Configuration Example

Host A connects port F0/10 of the switch. Host B connects port F0/12. The IP address of the radius-server host is 192.168.20.2. The key of radius is TST. Port F0/10 adopts remote radius authentication and user binding. Port F0/12 adopts local authentication of eap type, and Multi-hosts are enabled at Port F0/12.

Global configuration

username switch password 0 TST username TST password 0 TST
aaa authentication dot1x TST-F0/10 radius aaa authentication dot1x TST-F0/12 local interface VLAN1
ip address 192.168.20.24 255.255.255.0
radius-server host 192.168.20.2 auth-port 1812 acct-port 1813 radius-server key TST

Configuring port F0/10

interface FastEthernet0/10 dot1x port-control auto
dot1x authentication method TST-F0/10 dot1x user-permit radius-TST

Configuring port F0/12

interface FastEthernet0/12 dot1x multiple-hosts dot1x port-control auto
dot1x authentication method TST-F0/12 dot1x authentication type eap