# FSOS

# 802.1X Configuration

# Contents

# 1. 802.1X Configuration

## 1.1 802.1x Overview

IEEE 802.1X is the accessing management protocol standard based on interface accessing control passed in June, 2001. Traditional LAN does not provide accessing authentication. User can access the devices and resources in LAN when connecting to the LAN, which is a safety loophole. For application of mobile office and CPN, device provider hopes to control and configure user's connecting. There is also the need for accounting.

IEEE 802.1X is a network accessing control technology based on interface, which is the accessing devices authentication and control by physical accessing level of LAN devices. Physical accessing level here means the interface of LAN Switch devices. When authenticating, Switch is the in-between (agency) of client and authentication server. It obtains user's identity from client of accessing Switch and verifies the information through authentication server. If the authentication passes, this user is allowed to access LAN resources or it will be refused.

### 1.1.1 802.1x Authentication

802.1X operates in the typical client/server model and defines three entities: supplicant system, authentication system, and authentication server system:

- **Supplicant System**: It is required to access the LAN, and enjoy the services provided by the Switch equipment (such as PC), the client needs to support EAPOL agreement, and the client must run the IEEE 802.1X authentication client software.
- **Authentication System**: In the Ethernet system, the authentication Switch is mainly used to upload and deliver user authentication information and control whether the port is available according to the authentication result. As if between the client and the authentication server to act as a proxy role.
- **Authentication Server**: Normally refers to the RADIUS server. RADIUS checks the identity of the client (user name and password) to determine whether the user has the right to use the network system to provide network services. After the end of the authentication, results will be sent to the Switch.

Figure 1-1 shows the relationship between the three parts.

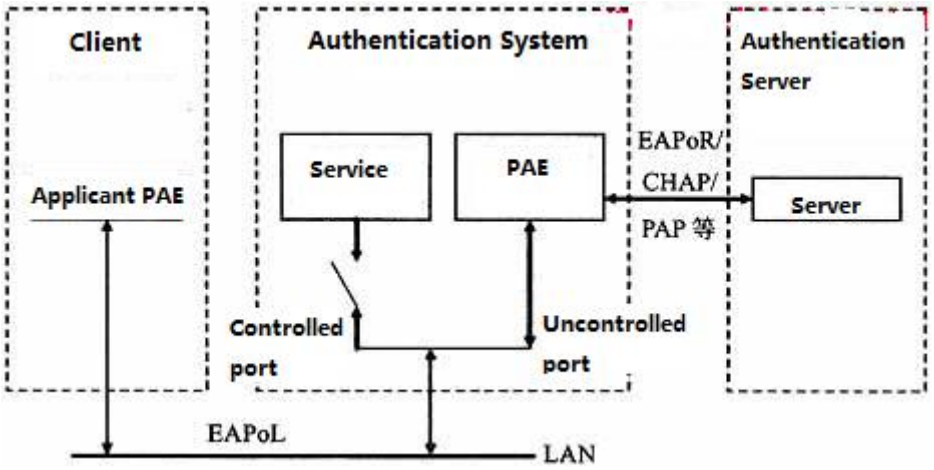



Figure 1-1 architecture of 802.1X

The above systems involve three basic concepts: PAE, controlled port, control direction:

1. PAE

Port Access Entity (PAE) refers to the entity that performs the 802.1x algorithm and protocol operations.

- PAE is the entity responsible for performing algorithms and protocol operations in the authentication mechanism. The PAE uses the authentication server to authenticate the clients that need to access the LAN, and controls the authorized / unauthorized status of the controlled ports accordingly according to the authentication result. The client PAE responds to the authentication request from the device and sends the user authentication information to the device. The client PAE can also send the authentication request and the offline request to the device.

2. Controlled port and uncontrolled port

An authenticator provides ports for supplicants to access the LAN. Each of the ports can be regarded as two logical ports: a controlled port and an uncontrolled port.

- The uncontrolled port is always enabled in both the ingress and egress directions to allow EAPOL protocol frames to pass, guaranteeing that the supplicant can always send and receive authentication frames.
- The controlled port is enabled to allow normal traffic to pass only when it is in the authorized state.
- The controlled port and uncontrolled port are two parts of the same port. Any frames arriving at the port are visible to both of them.

3. Control direction

In the non-authorized state, the controlled port is set to one-way controlled: the implementation of one-way controlled, prohibits the receiving frame from the client, but allows the client to send frames.

4． Port controlled manner

- Port-based authentication:

  As long as the first user authentication is successful under the physical ports, other access users without authentication can use the network source, when the first user is off line, other users will be refused to use network.

- MAC-address-based authentication:

  All the users on the physical port need to be authenticated separately. When userA goes offline, only the userA cannot use the network.

### 1.1.2 802.1x Authentication Process

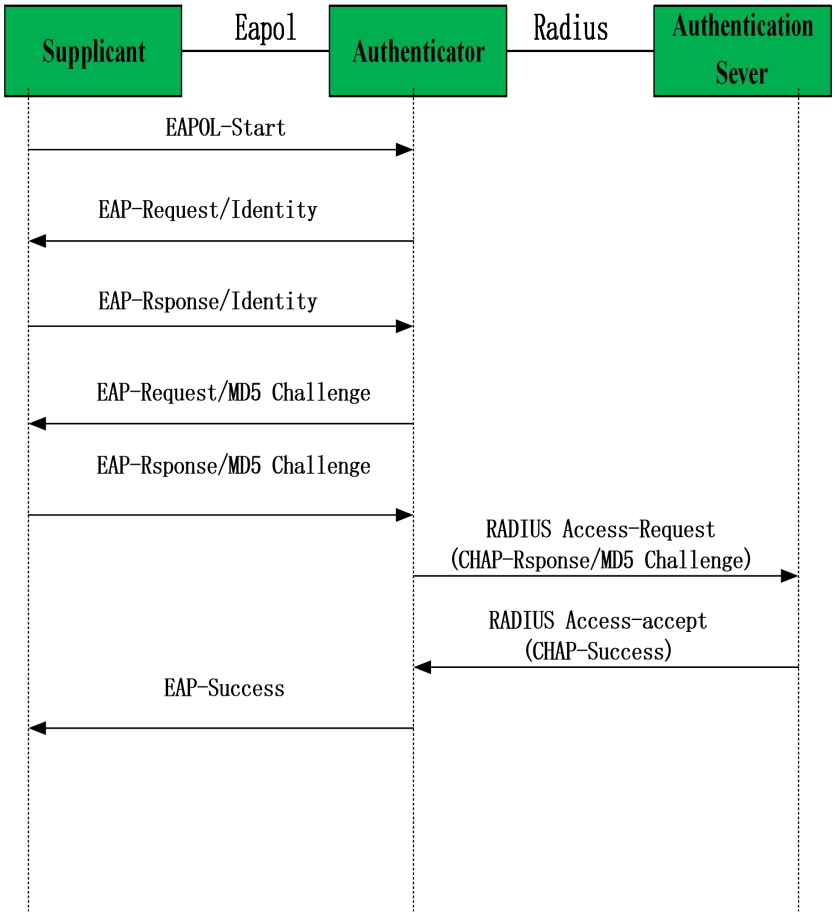
The 802.1x authentication system employs the Extensible Authentication Protocol (EAP) to exchange authentication information between the supplicant PAE, authenticator PAE, and authentication server.

At present, the EAP relay mode supports four authentication methods: EAP-MD5, EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled Transport Layer Security), and PEAP (Protected Extensible Authentication Protocol).

Switch supports EAP-Transfer mode and EAP-Finish mode to interactive with remote RADIUS server to finish the authentication.

1. EAP-Transfer

The following takes EAP-Transfer authentication process for an example to introduce the basic service procedure. As shown in the following:




EAP-Transfer authentication process

The authentication process is as follows:

(1) When the user needs to access the network, it will input the registered user name and password through the 802.1X client and initiate the connection request (EAPOL-Start packet). At this point, the client program will send the request message to the device, start an authentication process.;

(2) After receiving the requested data frame, the access device sends out a request frame (EAP-Request / Identity packet) to ask the user's client program for the user name;

(3) The client responds to the request from the device and sends the user name information to the device through the data frame (EAP-Response / Identity packet). The device encapsulates the RADIUS Access-Request packet and then sends it to the authentication server for processing after receiving the data frame packet from the client;

(4) After receiving the user name information from the device, the RADIUS server compares the information with the user name table in the database, finds the corresponding

password information, and encrypts it with a randomly generated encryption key. And it sends the encrypted keyword to the device through a RADIUS Access-Challenge packet. The message is then forwarded by the device to the client;

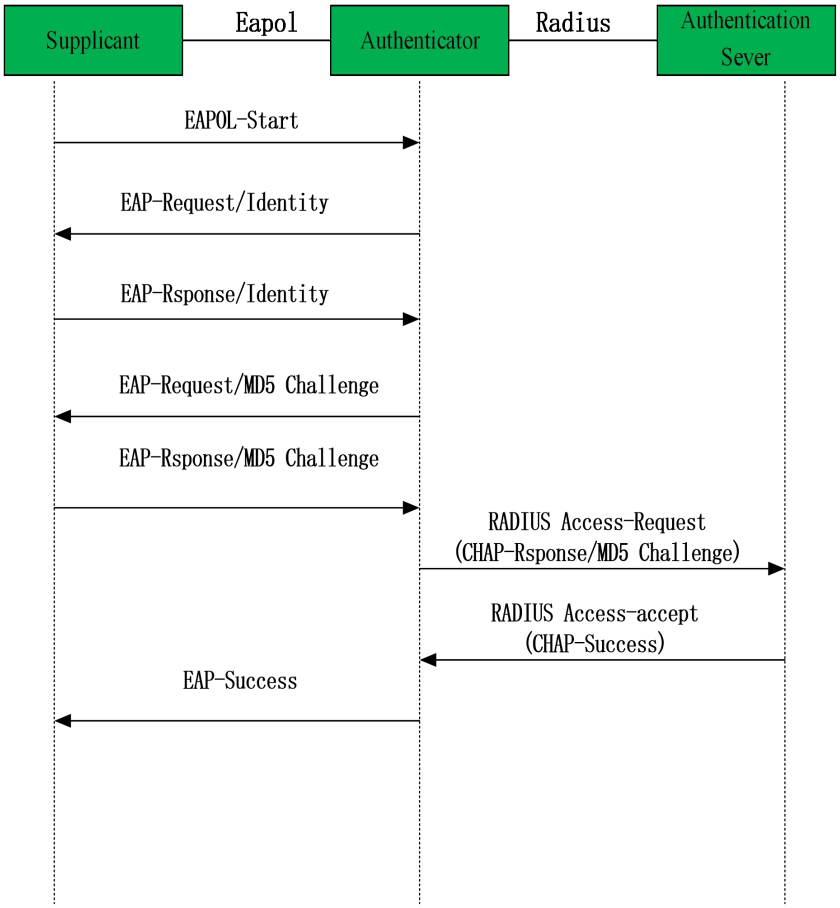
(5) After receiving the EAP-Request / MD5 Challenge packet, the client encrypts the encrypted part (this encryption algorithm is usually irreversible) and generates the EAP-Response / MD5 Challenge packets and pass the authentication packets to the authentication server.;

(6) The RADIUS server compares the received encrypted information (RADIUS Access-Request packet) with the local encrypted password information. If the password is the same, the RADIUS server considers the user to be a valid user and sends out the message -Accept and EAP-Success);

(7) After receiving the authentication message, the device changes the port to the authorized state, allowing the user to access the network through the port.

2. EAP-Finsh

In this way, EAP packets are terminated at the device end and are mapped to RADIUS packets. The RADIUS server uses the standard RADIUS protocol to complete authentication, authorization, and accounting. The PAP or CHAP authentication method can be adopted between the device and the RADIUS server. Our Switch defaults to this mode. The following takes the CHAP authentication method as an example to describe the basic service flow, as shown below:




EAP-Finish authentication process

The EAP termination mode differs from the authentication process of EAP relay mode in that a random encryption key for encrypting the user's password information is generated by the device, and then the device encrypts the user name, the random encryption key, and the encrypted password information of the client to the RADIUS server, and perform the related authentication process.

## 1.2 802.1X Configuration

### 1.2.1 Configure EAP

The 802.1x standard forwards the 802.1X authentication packets (Encapsulated with EAP frames) from the user to the RADIUS server without any processing. However, the traditional RADIUS server does not support the EAP feature. Therefore, the system supports the conversion of the authentication packets sent by the user to the data frames

encapsulated by the standard RADIUS protocol and then forwards the packets to the RADIUS server.

Configure EAP

| Operation | Command | Remarks |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Set the protocol interaction mode between the system and the RADIUS server | **dot1x { eap-finish \| eap-transfer }** | Optional eap-finish by default |

## 1.2.2 Enable 802.1x

802.1x provides a user identity authentication scheme. However, 802.1x cannot implement the authentication scheme solely by itself. RADIUS or local authentication must be configured to work with 802.1x.

After enabling the 802.1X, the users who connected to the system can access to the LAN resources only after it had passed the authentication. When enabling the 802.1X, you should point out the whether the enabling way is based on interface authentication or MAC address authentication. The interface which does not participate in 802.1X authentication has no need to enable 802.1X authentication.

1) Interface configuration based on interface authentication: if one of the users under the port had passed the authentication, other users can use the network resources without authentication; However, if that user who had passed the authentication logoff, other users can not be able to use the network resources.

Interface configuration based on MAC address authentication: each user under the port should perform separate authentication. Only the user who had passed the authentication can he use the network resources. If a certain user logoff, it cannot affect other authenticated users to use the network resources.

Enable 802.1x

| Operation | Command | Remarks |
|---|---|---|
| Enter global configuration | **configure terminal** | - |

| | | |
|---|---|---|
| mode | | |
| Enable 802.1x | **dot1x method { macbased \| portbased }** [ *interface-list* ] | required |

### 1.2.3 Configure 802.1x Parameters for a Port

After the interface enables the 802.1X authentication, this port needs to be authenticated by default while the uplink interface and the interface which connects to the server do not need, so you can configure the ports which do not need to be authenticated to be forceauthorized or disable their authentication functions. In addition, the interface which is banned to perform 802.1X authentication can be configured to be forceunauthorized.

Configure 802.1x Parameters for a Port

| Operation | Command | Remarks |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure 802.1x parameters for a port | **dot1x port-control** { **auto** \| **forceauthorized** \| **forceunauthorized** } [ *interface-list* ] | optional |

### 1.2.4 Re-authentication Configuration

In EAP-FINISH way, the port supports re-authentication. After the user is authenticated, the port can be configured to immediately re-certification, or periodic re-authentication.

re-authentication configuration

| Operation | Command | Remarks |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Immediately re-certification | **dot1x re-authenticate** [ *interface-list* ] | optional |
| Periodic re-authentication enabled on a port | **dot1x re-authentication** [ *interface-list* ] | optional |
| Periodic | **dot1x timeout re-authperiod** *time* [ *interface-list* ] | optional |

| | | |
|---|---|---|
| re-authentication time configuration port | | |

## 1.2.5 Watch Feature Configuration

After enabling this function, a port sends a 1x watch message periodically when no user is present, triggering the following users to perform 802.1x authentication.

This triggering method is used to support clients that cannot send EAPOL-Start packets, such as 802.1X clients. Our device sends an EAP-Request / Identity packet to the client every N seconds to trigger authentication.

Watch Feature Configuration

| Operation | Command | Remarks |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enable the watch function | **dot1x daemon** [ *interface-list* ] | optional |
| Configure the forwarding interval of watch packet | **dot1x daemon time** *time* [ *interface-list* ] | Optional 60S by default |
| Restore the default forwarding interval of watch packet | **no dot1x daemon time** [ *interface-list* ] | optional |

## 1.2.6 Configure User Features

The operations mainly perform the operations, for example, the configurations for number of port users, delete users, heartbeat detection operations, etc.

Heartbeat detection: After this function is enabled, the device periodically forwards EAP-Request/Identity to the client ports, the normal online client responds with the EAP-Rsponse/Identity. If the four consecutive EAP-Request/Identity packets are not received the EAP-Rsponse/Identity packet from the client, the device considers the user to go offline, and then it will delete the session and change the port to an unauthorized state.

Quiesce function: After the user authentication fails, the device needs to quiesce for a

period of time (The time can be configured through *dot1x quiet-period-value*. By default, no quiesced is required). During the quiesced period, the authenticator does not process the authentication request.

Configure User Features

| Operation | Command | Remarks |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the maximum number of users that can pass authentication | **dot1x max-user** *number* | optional |
| Delete the specified online user | **dot1x user cut** { **username** *name* \| **mac-address** *mac* } | optional |
| Enable heartbeat detection | **dot1x detect** [ *interface-list* ] | Optional 25s by default |
| Configure Heartbeat detection time | **dot1x detect interval** *time* | optional |
| Restore the default heartbeat detection time | **no dot1x detect interval** | optional |
| Configure the quiesce function | **dot1x quiet-period-value** *time* | Optional; 0 by default; No quiesce. |
| Restore the default quiet period value | **no dot1x quiet-period-value** | optional |

## 1.2.7 Configure Host Mode Based on Port Authentication Mode

The host mode configuration only takes effect in port authentication method, please configure the port as port-based authentication; if the configuration of the host mode is the single-host, configure the port to be mac-based authentication, host mode will automatically become invalid.

（1）multi-hosts: Multi-hosts mode, when a user authentication is passed on the port,

other users of the port can access network without authentication.

（2）single-host: Single-host mode, the user access network which the port allows only one authentication to pass and other users cannot access to the network, also can't go through authentication.

Configuration host-mode

| Operation | Command | Remarks |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure host-mode based on port authentication mode | **dot1x portbased host-mode { multi-hosts \| single-host }** [ *interface-list* ] | optional |

## 1.2.8 Configure Guest VLAN

After enabling 1X authentication, the user can access only the network resources of the VLAN when the guest VLAN is configured on the port. Once the user authentication succeeds, the port automatically reverts to the previously configured VLAN. If the authentication server delivers a valid VLAN, the port is automatically added to the assigned VLAN. After the user goes offline, the port reverts to the guest VLAN.

To ensure that all functions can be used normally, please assign different VLAN IDs for the Config VLAN, the radius distribution VLAN, and the Guest VLAN.

Guest VLAN configuration

| Operation | Command | Remarks |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure Guest VLAN | **dot1x guest-vlan** *vlan-id* [ *interface-list* ] | optional |

## 1.2.9 Configure Radius vlan

When 802.1X user pass the authentication via radius server, the server will transmit the authentication information to the device. If the device has enabled radius function and the

server has configured to distribute VLAN (adopting Tunnel-Pvt-Group-ID (81) attribute), the authentication information will include the distributed VLAN information as a consequence, what is more, the device will add the user authentication online interface to radius distributed VLAN.

Configure Radius vlan

| Operation | Command | Remarks |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter AAA configuration mode | **aaa** | |
| Enable radius vlan distribution function | **radius vlan enable** | Optional<br>Disabled by default |

🕮 **Note:**

Before using the radius vlan distribution function, you should create the corresponding VLAN and then add the user interface to the corresponding VLAN, so does Guest VLAN and Default-active-vlan；

Radius distributes VLAN, but it does not change the interface original VLAN configuration, so does Guest VLAN and Default-active-vlan.

As to the interface-based authentication and the MAC-based authentication, radius vlan ， Guest VLAN and Default-active-vlan are effective.

## 1.2.10 Configure EAPOL Transmission

When a port disables 802.1x authentication, it requires to transmit user 802.1x EAPOL message. So the equipment will work as the relay, users can perform 802.1x authentication in the upper equipment. This function can only handle EAPOL packet forwarded to CPU. For packets that do not forward to CPU, the packets are processed by the hardware and are not subject to this configuration. You can configure EAPOL transparent transmission port and the corresponding uplink port only when the 802.1x authentication is disabled. That is, you can not configure transparent transmission function when the 802.1x authentication is enabled.

Configure EAPOL Transmission

| Operation | Command | Remarks |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enable port EAPOL message transmission function | **dot1x eapol-relay** [ *interface-list* ] | optional |
| Configure EAPOL message transmission uplink port | **dot1x eapol-relay uplink** [ *interface-list* ] | optional |

## 1.2.11 Dot1x Display and Maintenance

Dot1x Display and Maintenance

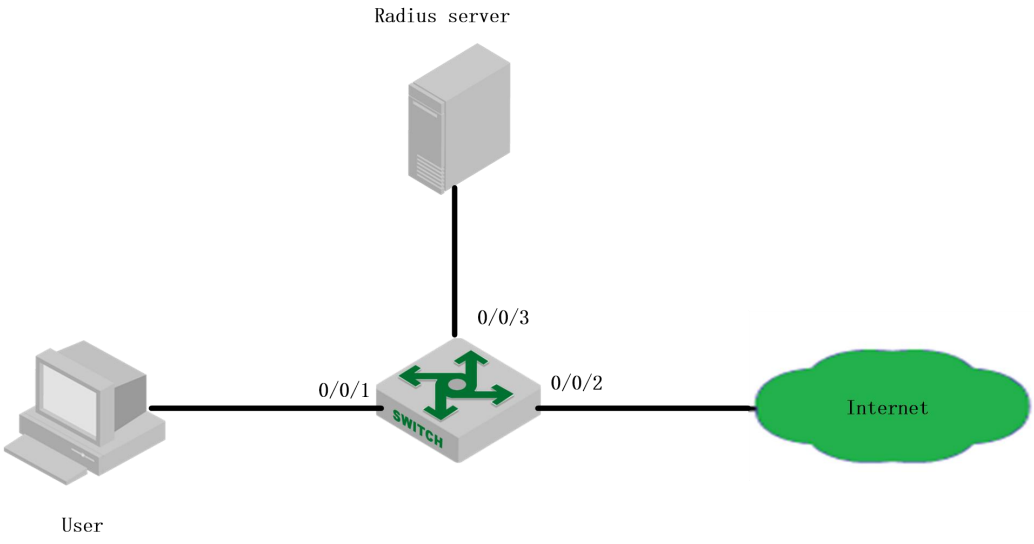
| Operation | Command | Remarks |
|---|---|---|
| Display the status of 802.1X authentication function | **show dot1x** | |
| Display the configuration of 802.1x authentication interface watch function | **show dot1x daemon [ interface** *interface-num* **]** | |
| Display interface configuration, such as the interface control mode, re-authentication state, the maximum number of users for the interface authentication. | **show dot1x interface [** *interface-num* **]** | |
| Display 802.1X session | **show dot1x session [ { interface** *interface-num* **} \| { mac-address** *mac* **} ]** | User online state (port number, VLAN ID, mac address, username, etc.) |

| | | |
|---|---|---|
| Display EAPOL pass through configuration | **show dot1x eapol-relay** **[ interface** *interface-num* **]** | |
| Display heartbeat detection configuration | **show dot1x detect [ interface** *interface-num* **]** | |
| Display guest-vlan information | **show dot1x guest-vlan [ interface** *interface-num* **]** | |
| Display whether the interface authentication is enabled or disabled | **show dot1x port-auth** | |
| Display quiet period | **show dot1x quiet-period-value** | |
| Debug DOT1X receive packet and transmit packet as well as module processing | **debug dot1x** | |

## 1.3 Configuration Example

### 1.3.1 Networking Requirements

Local 802.1 x access user name is u1, and then password is 123. User can be able to access internet after login successfully. Network diagram are shown below:



network diagram of 802.1X configuration

## 1.3.2 Configuration steps

1) Enable the 802.1x authentication of Ethernet port 0/0/1

Switch(config)#dot1x method macbased interface ethernet 0/0/1

2) Configure the basic function of RADIUS server（create RADIUS 1， configure the master authentication server to be 1.1.1.1, primary accounting server to be 1.1.1.2, the authentication shared key and accounting shared key to be 123456. Please refer to 《Radius configuration 》for more RADIUS detailed configuration. )

Switch(config-aaa)#radius host 1
Switch(config-aaa-radius-1)#primary-auth-ip 1.1.1.1 1812
Switch(config-aaa-radius-1)#primary-acct-ip 1.1.1.2 1813
Switch(config-aaa-radius-1)#auth-secret-key 123456
Switch(config-aaa-radius-1)#acct-secret-key 123456
Switch (config-aaa)#domain abc.com
Switch (config-aaa-domain-abc.com)#radius host binding 1
Switch (config-aaa-domain-abc.com)#state active
Switch(config-aaa)#default domain-name enable abc.com

## 1.3.3 Result validation

User inputs the username and password on the 802.1X client to perform authentication. Through the command of "show dot1x session", it shows the current user had passed the authentication and login successfully, that is to say, the user can be able to access the internet.

Switch(config)#show dot1x session

| port | vid | mac | username | login time |
|---|---|---|---|---|
| 0/0/1 | 1 | c8:3a:35:d3:e3:99 | u1@abc.com | 2000/01/01 05:13:42 |