

DIGISOL[®]

802.1x Configuration

As our products undergo continuous development the specifications are subject to change without prior notice.

Table of Contents

| | |
|---|---|
| Chapter 1 Configuring 802.1x..... | 1 |
| 1.1 802.1x Configuration Task List | 1 |
| 1.2 802.1x Configuration Task | 1 |
| 1.2.1 Configuring 802.1x Port Authentication | 1 |
| 1.2.2 Configuring 802.1x Multiple Port Authentication | 2 |
| 1.2.3 Configuring 802.1x Re-authentication..... | 3 |
| 1.2.4 Configuring 802.1x Re-authentication times | 3 |
| 1.2.5 Configuring 802.1x Transmission Frequency..... | 3 |
| 1.2.6 Configuring 802.1x User Binding | 4 |
| 1.2.7 Configuring Authentication Method for 802.1x Port..... | 4 |
| 1.2.8 Selecting Authentication Type for 802.1x Port..... | 4 |
| 1.2.9 Configuring MAB Authentication on the Port..... | 5 |
| 1.2.10 Configuring 802.1x Accounting | 5 |
| 1.2.11 Configuring 802.1x guest-vlan..... | 6 |
| 1.2.12 Forbidding Supplicant With Multiple Network Cards | 6 |
| 1.2.13 Resuming Default 802.1x Configuration..... | 6 |
| 1.2.14 Monitoring 802.1x Authentication Configuration and State | 7 |
| 1.3 802.1x Configuration Example | 7 |



Chapter 1 Configuring 802.1x

1.1 802.1x Configuration Task List

- Configuring 802.1x port authentication
- Configuring 802.1x multiple port authentication
- Configuring 802.1x re-authentication
- Configuring 802.1x re-authentication times
- 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 port mab authentication
- Configuring 802.1x accounting
- Configuring 802.1x 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 data 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:

| Command | Purpose |
|---------------------|-----------------------------|
| dot1x enable | Enable the 802.1x function. |

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

| Command | Purpose |
|--|---|
| dot1x port-control auto | Configure the 802.1x protocol control method on the port. |
| aaa authentication dot1x {default list name} method1 [method2...] | Configure the AAA authentication of 802.1x. |

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

| Command | Purpose |
|--|---|
| dot1x port-control auto | Enables 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. |
| dot1x port-control misc-mab | Enables 802.1x hybrid 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.

The multi-auth has two modes: one is multiple-host mode and the other is multiple-auth mode. In **multiple-hosts** mode, the port will be set to **up** if one of the users passes the authentication. Thus, other users can access the device by the port without authentication. In **multiple-auth** mode, the switch will authenticate each user separately. The port will be set to **up** if one user has been successfully authenticated. The port is set to down if all users are failed to authenticate. Thus, the failure of one user will not affect other users' access to the device.



Note: **Multi-auth** mode cannot be configured simultaneously with **guest vlan** or **mab authentication**. 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 802.1x multiple host authentication:

| Command | Purpose |
|--|---|
| dot1x authentication multiple-hosts | Set the 802.1x multiple port authentication. The port is set to up only if one user passes the authentication. |
| dot1x authentication multiple-auth | Set the 802.1x multiple port authentication. Each user is non-related in authentication. |

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 | To |
|--|--|
| dot1x re-authentication | Enables the re-authentication function. |
| dot1x timeout re-authperiod <i>time</i> | Configures the period of the re-authentication function. |

1.2.4 Configuring 802.1x Re-authentication times

After the authentication fails, the switch will re-send request/ID packet to enable the authentication. When the re-authentication times exceeds the certain number and there is still no respond, the authentication will be suspended.

Run the following command in interface configuration command to set the maximum times for of re- authentication:

| Command | Purpose |
|-------------------------------------|--|
| dot1x reauth-max <i>time</i> | Set the maximum times of re- authentication. |

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:



| Command | Purpose |
|--|---|
| dot1x timeout tx-period <i>time</i> | 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.

| Command | Purpose |
|--------------------------------------|---|
| dot1x user-permit <i>xxxz</i> | 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:

| Command | Purpose |
|---|--|
| dot1x authentication method <i>yyy</i> | 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:

| Command | Purpose |
|-------------------------------------|---------------------|
| dot1x authen-type {chap eap} | Select chap or eap. |

Also run the following command in interface configuration mode:

| Command | Purpose |
|---------|---------|
|---------|---------|



| | |
|---|--|
| dot1x authentication type {chap eap} | Select chap or eap or the configured authentication type 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 MAB 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 the peer device not to support the 802.1x authentication client and then turns to the MAB authentication.

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

When the MAB authentication is enabled, you can set the format of the MAC address to the Radius server through this command.

| 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 six formats from format 1 to format 6. The default format is 1. |

1.2.10 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:

| Command | Purpose |
|--|--|
| dot1x accounting enable | Enable the dot1x accounting. |
| dot1x accounting method {method name} | Configure the accounting method. Its default value is default . |

1.2.11 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:

| Command | Purpose |
|-------------------------|-------------------------------------|
| Dot1x guest-vlan | Enable the guest-vlan at all ports. |

When there is no **guest-vlan id** originally configured at each port, 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**:

| Command | Purpose |
|--------------------------------------|--|
| Dot1x guest-vlan {id(1-4094)} | Enable the vlan id of guest-vlan at all ports. |

1.2.12 Forbidding Supplicant With Multiple Network Cards

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

| Command | Purpose |
|---|---|
| dot1x forbid multi-network-adapter | Forbid the Supplicant with multiple network adapters. |

1.2.13 Resuming Default 802.1x Configuration

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

| Command | Purpose |
|---------|---------|
|---------|---------|



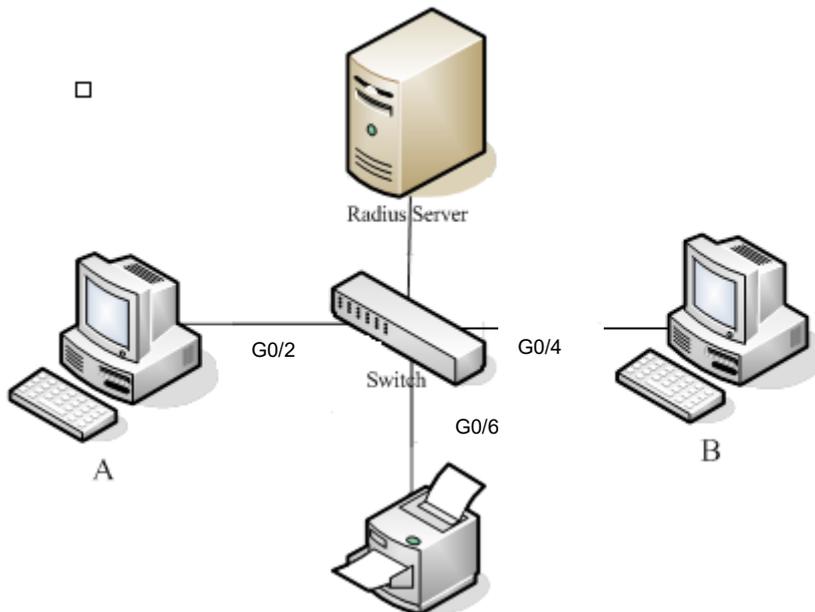
| | |
|----------------------|---|
| dot1x default | Resume all global configuration to default configuration. |
|----------------------|---|

1.2.14 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:

| Command | Purpose |
|---|---|
| show dot1x { interface statistics misc-mab-db } | Monitor the configuration and state of 802.1x authentication. |

1.3 802.1x Configuration Example



Host A connects port G0/2 of the switch. Host B connects port G0/4. Host C connects with port G0/6. The IP address of the radius-server host is 192.168.20.2. The key of radius is TST. Port G0/2 adopts remote radius authentication, user binding and re-authentication. Port G0/4 adopts local authentication of eap type, and enables multi-host and guest-vlan. Port G0/6 adopts mab authentication and the 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
```

Configuring port G0/2

```
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
```

Configuring port G0/4

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

Configuring port G0/6

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

