802.1x Configuration Commands

Table of Contents

Chapter 1 802.1x Configuration Commands 1
1.1 802.1x Configuration Commands 1
1.1.1 dot1x enable 2
1.1.2 dot1x port-control 2
1.1.3 dot1x authentication multiple-hosts 3
1.1.4 dot1x authentication multiple-auth 4
1.1.5 dot1x default 5
1.1.6 dot1x reauth-max 6
1.1.7 dot1x re-authentication 7
1.1.8 dot1x timeout quiet-period 7
1.1.9 dot1x timeout re-authperiod 8
1.1.10 dot1x timeout tx-period 9
1.1.11 dot1x mab 10
1.1.12 dot1x mabformat 11
1.1.13 dot1x user-permit 11
1.1.14 dot1x authentication method 12
1.1.15 dot1x accounting enable 13
1.1.16 dot1x accounting method 14
1.1.17 dot1x authen-type、 dot1x authentication type 15
1.1.18 dot1x guest-vlan 16
1.1.19 dot1x guest-vlan id 17
1.1.20 dot1x forbid multi-network-adapter 18
1.1.21 aaa authentication dot1x 19
1.1.22 debug dot1x error 19
1.1.23 debug dot1x state 20
1.1.24 debug dot1x packet 21
1.1.25 show dot1x 21

Chapter 1 802.1x Configuration Commands

1.1 802.1x Configuration Commands

The following commands are used to configure 802.1x:

- dot1x enable
- dot1x port-control
- dot1x authentication multiple-hosts
- dot1x authentication authentication
- dot1x default
- dot1x max-req
- dot1x reauth-max
- dot1x re-authentication
- dot1x timeout quiet-period
- dot1x timeout re-authperiod
- dot1x timeout tx-period
- dot1x mab
- dot1x mabformat
- dot1x user-permit
- dot1x authentication method
- dot1x accounting enable
- dot1x accounting method
- dot1x authen-type、dot1x authentication type
- dot1x guest-vlan
- dot1x guest-vlan id
- dot1x forbid multi-network-adapter
- aaa authentication dot1x
- debug dot1x error

- debug dot1x state
- debug dot1x packet
- show dot1x

1.1.1 dot1x enable

Syntax

dot1x enable

no dot1x enable

Parameter

None

Default value

None

Instruction

If the 802.1x function is not enabled, you cannot start it on an interface. If the 802.1x function is forbidden, all interfaces have no the 802.1x function, and at the same time, all 802.1x packets will not be received by CPU but can be forwarded in VLAN like normal multicast packets.

Command mode

Global configuration mode

Example

The following example shows how to enable dot1x.

```
Switch_config#dot1x enable
Switch_config#
```

1.1.2 dot1x port-control

Syntax

dot1x port-control {***auto***|***force-authorized***|***force-unauthorized***}

no dot1x port-control

Parameter

Parameter	Description
auto	Enables the 802.1x authentication mode.
force-authorized	Cancels the 802.1x authentication.
force-unauthorized	Sets the interface to **unauthorized** mandatorily.

Default value

force-authorized

Instruction

The 802.1x protocol is an interface-based two-layer authentication mode. You can run the **auto** command to enable the authentication mode. This authentication mode can be configured only on the physical interface and the interface's attributes cannot include VLAN backbone, dynamical access, security port or listening port.

Command mode

Port configuration mode

Example

The following example shows how to enable 802.1x on interface f0/24.

Switch_config_f0/24# dot1x port-control auto
Switch_config_f0/24#

The following example shows how to firstly set interface f0/23 to the VLAN backbone and then enable 802.1x.

Switch_config_f0/23switchport mode trunk
Switch_config_f0/23dot1x port-control auto
802.1x Control Failed, 802.1x cannot cmd on vlanTrunk port(f0/23)
Switch_config_f0/23

1.1.3 dot1x authentication multiple-hosts

Syntax

dot1x authentication multiple-hosts

no dot1x authentication multiple-hosts

Parameter

None

Default value

The 802.1x multi-client authentication is disabled.

Instruction

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.

When you set 802.1x multi-host authentication on an interface, the switch will take authentication towards to different hosts, and when a host's authentication passes, the interface will be in UP state and then the remaining hosts (including the previous hosts and the following ones) need not be authenticated.

Note: If an interface is in multi-host mode, all users on the interface will be authenticated again.

Command mode

Port configuration mode

Example

The following example shows how to enable multi-host authentication on interface f0/24.

Switch_config_f0/24#dot1x authentication *multiple-hosts*

Switch_config_f0/24#

1.1.4 dot1x authentication multiple-auth

Syntax

dot1x authentication multiple-auth

no dot1x authentication multiple-auth

Parameter

None

Default value

The 802.1x multi-client authentication is disabled.

Instruction

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.

When an interface is set to 802.1x multiple-auth, the switch will conduct authentication towards to all host users. The switch will authenticate each host users respectively but the authentication of one host user does not interfere with others' authentication, that is, the present authentication would not interfere with the previous or following ones. 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-authen mode, all users on the interface will be authenticated again.

Command mode

Port configuration mode

Example

The following example shows how to enable multiple-authentication on interface f0/24.

Switch_config_f0/23# dot1x authentication *multiple-hosts*
Switch_config_f0/23#

1.1.5 dot1x default

Syntax

dot1x default

Parameter

None

Default value

None

Instruction

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

Command mode

Global configuration mode

Example

The following example shows how to resume all dot1x configuration parameters to their default values.

Switch_config#dot1x *default*
Switch_config#

1.1.6 dot1x reauth-max

Syntax

dot1x reauth-max *count*

no dot1x reauth-max

Parameter

Parameter	Description
count	Maximum authentication re-try times, ranging between 1 and 10

Default value

4

Instruction

This command is used to set the authentication retry times. If the retry times exceeds the maximum retry times and the client has no response, the authentication is mounted.

Command mode

Global configuration mode

Example

The following example shows how to configure the maximum times of dot1x identity authentication request to **5**.

Switch_config#dot1x *reauth-max 5*
Switch_config#

1.1.7 dot1x re-authentication

Syntax

dot1x re-authentication

no dot1x re-authentication

Parameter

None

Default value

None

Instruction

After an interface passes authentication, the interface will still perform authentication to hosts in a certain period. You can run **dot1x timeout re-autjperiod** to configure the period.

Command mode

Global configuration mode

Example

The following example shows how to enable the re-authentication function.

Switch_config#dot1x *re-authentication*
Switch_config#

1.1.8 dot1x timeout quiet-period

Syntax

dot1x timeout quiet-period *time*

no dot1x timeout quiet-period

Parameter

Parameter	Description
time	Period for restarting dot1x authentication, ranging between 0 and 65535 seconds

Default value

60s

Instruction

There is a certain period when the switch cannot perform any authentication after the previous authentication fails.

Command mode

Global configuration mode

Example

The following example shows how to set the value of **quiet-period** to 40.

Switch_config#dot1x *timeout quiet-period 40*
Switch_config#

1.1.9 dot1x timeout re-authperiod

Syntax

dot1x timeout re-authperiod *time*

no dot1x timeout re-authperiod

Parameter

Parameter	Description
time	dot1x re-authentication period, ranging between 1 and 4294967295s

Default value

3600s

Instruction

This command validates only when the re-authentication function is enabled.

Command mode

Global configuration mode

Example

The following example shows how to set the dot1x re-authentication period to 7200 seconds.

Switch_config#dot1x *timeout re-authperiod 7200*
Switch_config#

1.1.10 dot1x timeout tx-period

Syntax

dot1x timeout tx-period *time*

no dot1x timeout tx-period

Parameter

Parameter	Description
time	Time which ranges between 1 and 65535 seconds

Default value

30s

Instruction

This command is used to set the client's authentication request response interval. If the interval is exceeded, the switch would retransmit the authentication request.

Command mode

Global configuration mode

Example

The following example shows how to set the transmission frequency to 24.

Switch_config_f0/23#dot1x *timeout tx-period 24*

Switch_config_f0/23#

1.1.11 dot1x mab

Syntax

dot1x mab

no dot1x mab

Parameter

None

Default value

The debugging switch is shut down.

Instruction

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.

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 supporting 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.

Command mode

Port configuration mode

Example

The following example shows how to enable mab authentication on port f0/1.

Switch_config_f0/1# dot1x *mab*
Switch_config_f0/1#

1.1.12 dot1x mabformat

Syntax

dot1x mabformat {**1**|**2**|**3**|**4**|**5**|**6**}

no dot1x mabformat

Parameter

Parameter	Description
1	Format of the MAC address: aa:bb:cc:dd:ee:ff
2	Format of the MAC address: AA:BB:CC:DD:EE:FF
3	Format of the MAC address: aabbccddeeff
4	Format of the MAC address: AABBCCDDEEFF
5	Format of the MAC address: aa-bb-cc-dd-ee-ff
6	Format of the MAC address: AA-BB-CC-DD-EE-FF

Default value

1

Instruction

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

Command mode

Global configuration mode

Example

The following example shows how to set the format of MAC to 3.

Switch_config# dot1x *mabformat 3*
Switch_config#

1.1.13 dot1x user-permit

Syntax

dot1x user-permit xxx yyy zzz

no dot1x user-permit

Parameter

Parameter	Description
xxx	A user name
yyy	A user name
zzz	A user name

Default value

No user is bound and all users would pass.

Instruction

This command can be used to bind users on an interface. Each interface can be bound to up to eight users. When the 802.1x authentication is enabled, the authentication is performed only to those bound users. However, to those unbound users, the authentication must fail.

Command mode

Port configuration mode

Example

The following example shows how to bind users a, b, c and d on interface f0/1.

Switch_config_f0/1#*dot1x user-permit a b c d*

Switch_config_f0/1#

1.1.14 dot1x authentication method

Syntax

dot1x authentication method xxx

no dot1x authentication method

Parameter

Parameter	Description
xxx	Method name

Default value

Default method

Instruction

This command is used to configure the authentication method which must be one of authentication methods provided by AAA. One interface only uses one authentication method. When AAA performs authentication to the 802.1x user, AAA would select the configured authentiction method to perform the authentication.

Command mode

Port configuration mode

Example

The following example shows how to set the authentication method on interface f0/1 to **abcd** which applies the local username for authentication and that on interface f0/2 to **efgh** which applies the remote radius authentication.

Switch_config #aaa authentication dot1x abcd local
Switch_config #aaa authentication dot1x efgh radius
Switch_config #int f0/1
Switch_config_f0/1# dot1x authentication method abcd
Switch_config_f0/1# int f0/2
Switch_config_f0/2# dot1x authentication method efgh

1.1.15 dot1x accounting enable

Syntax

dot1x accounting enable

no dot1x accounting enable

Parameter

Parameter	Description
None	

Default value

The accounting service is disabled by default.

Instruction

This command is used to enable the accounting function on a port which runs with the authentication function. You'd better enable the dotx re-authentication function when the accounting function is running.

Command mode

Port configuration mode

Example

The following example shows how to configure the dot1x authentication function on interface f0/1 and enable the accounting function.

Switch_config)#dot1x enable
Switch_config)#int f0/1
Switch_config_f0/1# dot1x port atuo
Switch_config_f0/1# dot1x accounting enable

1.1.16 dot1x accounting method

Syntax

dot1x accounting method xxx

no dot1x accounting method

Parameter

Parameter	Description
xxx	Name of the accounting method

Default value

Default method

Instruction

This command is used to configure an accounting method on a port. This method must be one of the accounting methods provided by AAA. Each port has only one accounting method. When the dot1x accounting function is enabled, this method will be used for accounting.

Command mode

Port configuration mode

Example

The following example shows how to set the accounting method on interface f0/1 to **abcd**, which uses the radius server.

Switch_config # aaa accounting network abcd start-stop group radius

Switch_config #radius host 192.168.20.100

Switch_config#int f0/1

Switch_config_f0/1# dot1x accounting method abcd

1.1.17 dot1x authen-type、dot1x authentication type

Syntax

dot1x authen-type {**chap**|**eap**}

no dot1x authen-type

To configure the dot1x authentication type in global configuration mode, run **dot1x authen-type**; to resume the default settings in global configuration mode, run **no dot1x authen-type**.

dot1x authentication type {**chap**|**eap**}

no dot1x authentication type

To configure the dot1x authentication type on an interface, run **dot1x authentication type**; to resume the default settings on an interface, run **no dot1x authentication type**.

Parameter

None

Default value

The default dot1x authentication type is **chap**.

The default dot1x authentication type in global configuration mode is also used applied by default in interface configuration mode.

Instruction

This command is used to configure the authentication class, while 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 alwayls used on the

interface unless the negative form of the command is run to resume the default settings.

Command mode

Interface or global configuration mode

Example

The following example shows how to set the authentication type on interface f0/1 to **chap** and the global authentication type to **eap**.

Switch_config #dot1x *authen-type eap*

Switch_config)#int f0/1

Switch_config_f0/1# dot1x authentication type chap

1.1.18 dot1x guest-vlan

Syntax

dot1x guest-vlan

no dot1x guest-vlan

To enable the guest-vlan function of dot1x in global configuration mode, run **dot1x guest-vlan. To disable the** guest-vlan function of dot1x in global configuration mode, run **no dot1x guest-vlan.**

Parameter

None

Default value

The guest-vlan function of dot1x is shut down in global configuration mode by default.

Instruction

After the guest-vlan function is enabled, the corresponding port can be grouped into the guest vlan and specific network access rights are attributed to the port if a guest terminal does not respond.

This command is used together with the **dot1x guest-vlan id** command.

Note: This command cannot be set together with the **multiple-auth** command.

Command mode

Global configuration mode

Example

The following example shows how to enable the guest-vlan function in global configuration mode.

Switch_config#dot1x guest-vlan

1.1.19 dot1x guest-vlan id

Syntax

dot1x guest-vlan id

no dot1x guest-vlan

To configure the value of **dot1x guest-vlan id** on an interface, run **dot1x guest-vlan id**; to resume the default value **0**, run **no dot1x guest-vlan**.

Parameter

ID: stands for the value of guest vlan, which can be any vlan ID configured in the system.

Default value

0

Instruction

After the guest-vlan function is enabled, the corresponding port can be grouped into the guest vlan and specific network access rights are attributed to the port if a guest terminal does not respond.

This command is used together with the **dot1x guest-vlan id** command.

Note: not with mutipie-auth command to configure the same time.

Command mode

Port configuration mode

Example

The following example shows how to configure the guest-vlan id in port configuration commands.

Switch_config_f0/23# 1dot1x guest-vlan 2

1.1.20 dot1x forbid multi-network-adapter

Syntax

dot1x forbid multi-network-adapter

no dot1x forbid multi-network-adapter

To forbid the supplicant of the multi-network-adapter on an interface, run **dot1x forbid multi-network-adapter. To resume the default settings, run no dot1x forbid multi-network-adapter.**

Parameter

None

Default value

None

Instruction

This command can be used to forbid the supplicant terminal with multiple network adapters, preventing an agent from being occurred.

Command mode

Port configuration mode

Example

The following example shows how to forbid the supplicant terminal with multiple network adapters in port configuration mode.

Switch_config_f0/23# dot1x forbid multi-network-adapter

1.1.21 aaa authentication dot1x

Syntax

aaa authentication dot1x {**default**} *method1* [*method2...*]

no aaa authentication dot1x {**default**} *method1* [*method2...*]

Parameter

Parameter	Description
default	Uses the following method when a user is authenticated.
method1 [*method2...*]	enable 、group radius、line、local、local-case、none

Default value

There is no authentication.

Instruction

The **method** parameter provides a series of methods to authenticate the password of the client host. You'd better adopt the radius as the AAA authentication mode of 802.1x. You can also use the local configuration data for authentication, such as user password saved in the local configuration.

Command mode

Global configuration mode

Example

The following example shows how to configure the dot1x authentication method to **radius**.

```
Switch_config#aaa authentication dot1x default radius
Switch_config#
```

1.1.22 debug dot1x error

Syntax

debug dot1x error

Parameter

None

Default value

None

Instruction

This command is used to export all error information occurred during dot1x running. The error information can help locating the errors.

1.1.23 debug dot1x state

Syntax

debug dot1x state

Parameter

None

Default value

None

Instruction

The following shows the format of information output:

2003-3-18 17:40:09 802.1x:AuthSM(F0/10) state Connecting-> Authenticating, event rxRespId

2003-3-18 17:40:09 802.1x:F0/10 Create user for Enter authentication

2003-3-18 17:40:09 802.1x:BauthSM(F0/10) state Idle-> Response, event authStart

2003-3-18 17:40:09 802.1x:F0/10 user "myname" denied, Authentication Force Failed

2003-3-18 17:40:09 802.1x:F0/10 Authentication Fail

2003-3-18 17:40:09 802.1x:BauthSM(F0/10) state Response-> Fail, event aFail

1.1.24 debug dot1x packet

Syntax

debug dot1x packet

Parameter

None

Default value

None

Instruction

2003-3-18 17:40:09 802.1x:F0/10 Tx --> Supplicant(0008.74bb.d21f)
EAPOL ver:01, type:00, len:5
EAP code:01, id:03, type:01, len:5
00
2003-3-18 17:40:09 802.1x:F0/10 Rx <-- Supplicant(0008.74bb.d21f)
EAPOL ver:01, type:00, len:10
EAP code:02, id:03, type:01, len:10
62 64 63 6f 6d a5

1.1.25 show dot1x

Syntax

show dot1x [interface *intf-id*]

To display the 802.1x configuration information, run the previous command.

Parameter

Parameter	Description
intf-id	Stands for a specific physical interface.

Default value

None

Instruction

This command is used to display the 802.1x configuration information.

Command mode

EXEC

Example

The following example shows how to configure **dot1x port-control auto** on interface f0/10.

```
Switch_config#sho dot1x
802.1X Parameters
reAuthen          No
reAuth-Period     3
quiet-Period      10
Tx-Period         30
Supp-timeout      30
Server-timeout    30
reAuth-max        4
max-request       2
authen-type       Eap
IEEE 802.1x on port F0/10 enabled
Authorized                  Yes
Authen Type                 Eap
Authen Method               default
Permit Users                All Users
Multiple Hosts              Disallowed
Supplicant                  aaa(0008.74bb.d21f)
Current Identifier          21
Authenticator State Machine
State                   Authenticated
Reauth Count                0
Backend State Machine
State                   Idle
Request Count               0
Identifier (Server)         20
Port Timer Machine
Auth Tx While Time          16
Backend While Time          16
reAuth Wait Time            3
Hold Wait Time              0
```