802.1x Configuration Commands

level one

Table of Contents

Chapter 1 802.1x Configuration Commands

1.1 802.1x Configuration Commands

802.1x configuration commands include:

- dot1x enable
- dot1x port-control
- dot1x authentication multiple-hosts
- dot1x authentication multiple-auth
- dot1x default
- 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 guest-vlan
- dot1x guest-vlan id
- dot1x forbid multi-network-adapter
- dot1x keepalive
- aaa authentication dot1x
- debug dot1x errors
- debug dot1x state
- debug dot1x packet
- show dot1x

1.1.1 dot1x enable

Syntax

dot1x enable
no dot1x enable

Parameter

None

Default

None

Usage Guidelines

Use this command to enable 802.1x feature. The 802.1x feature cannot be enabled on an interface. If 802.1x feature is disabled, then all 802.1x packets will be forwarded like other multi-cast packets in VLAN rather than be received by CPU.

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 802.1x protocol authentication method
force-authorized	Forced port authentication passed.
force-unauthorized	Forced port authentication failed.

Default

force-authorized

Usage Guidelines

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

Interface configuration mode

Example

The following example enables 802.1x on interface g0/0/1

```
Switch(config-g0/0/1)# dot1x port-control auto
Switch(config-g0/0/1)#
```

The following example configures interface g0/0/1 as the vlan trunk port and enables 802.1x:

```
Switch(config-g0/0/1)#switchport mode trunk
Switch(config-g0/0/1)#dot1x port-control auto
802.1x Control Failed, can't config 802.1x on vlanTrunk port(GigaEthernet0/1)
Switch(config-g0/0/1)#
```

1.1.3 dot1x authentication multiple-hosts

Syntax

dot1x authentication multiple-hosts
no dot1x authentication multiple-hosts

Parameter

None

Default

Disable the multiple authentication of 802.1x.

Usage Guidelines

Set one port to the multi-hosts mode of 802.1x, and the switch will authenticate different users. When one user passes the authentication, the port sets to the "up" state. Other users can access the port without authentication.

Note: After modifying the multi-host authentication mode, all users of the port will be authenticated again.

Command Mode

Interface configuration mode

Example

The following example enables multiple-hosts authentication on interface g0/0/1:

```
Switch(config-g0/0/1)# dot1x authentication multiple-hosts
Switch(config-g0/0/1)#
```

1.1.4 dot1x authentication multiple-auth

Syntax

dot1x authentication multiple-auth
no dot1x authentication multiple-auth

Parameter

None

Default

Disable the multiple authentication of 802.1x.

Usage Guidelines

After set one interface to the multiple-auth mode of 802.1x, the switch will set authentication for each user. The authentication for each user is unrelated. The interface shows “up” only when one user is successfully authenticate; the interface shows “down” when all users fail to authenticate. Thus, each user is respectively authenticated and any user’s failure of authentication has no effect on the authority of other users.

Note: The multi-auth mode cannot be configured with guest vlan, nor with mab. To modify the multi-host mode, all user need to be re-authenticated.

Command Mode

Interface configuration mode

Example

The following example shows how to enable multiple-auth in interface g0/0/1:

```
Switch(config-g0/0/1)# dot1x authentication multiple-auth
Switch(config-g0/0/1)#
```

1.1.5 dot1x default

Syntax

dot1x default

Parameter

None

Default

None

Usage Guidelines

The command is used to return all configuration to the default setting.

Command Mode

Global Configuration Mode

Example

The command shows how to return all configurations of dot1x to the default setting.

```
Switch(config)#dot1x default
Switch(config)#
```

1.1.6 dot1x reauth-max

Syntax

dot1x reauth-max *count*
no dot1x reauth-max

Parameter

Parameter	Syntax
count	Maximum number of retries. The value is from 1 to 10.

Default

5

Usage Guidelines

Use this command to set maximum number of re-authentications. The authentication will be suspended when there is no response from client on exceeding the number of this configured re-authentication times.

Command Mode

Global configuration mode

Example

The following example set 4 as the maximum number of re-authentications:

```
Switch(config)#dot1x reauth-max 4
Switch(config)#
```

1.1.7 dot1x re-authentication

Syntax

dot1x re-authentication
no dot1x re-authentication

Parameter

None

Default

None

Usage Guidelines

You configure the amount of time between the periodic re-authentication attempts by using the **dot1x timeout re-authperiod** global configuration command.

Command Mode

Global configuration mode

Example

This example shows how to enable the periodic re-authentication:

```
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	Syntax
time	Period of re-enabling authentication, in the range from 0 to 65535 seconds

Default

60s

Usage Guidelines

There will be a period of quiet time after authentication failure during which switch doesn't receive or enable any authentication.

Command Mode

Global configuration mode

Example

The following example configures quiet period value 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	Period of re-authentication, in the range from 1 to 600000s

Default

3600s

Usage Guidelines

This command is valid only after enabling the dot1x re-authentication command.

Command Mode

Global configuration mode

Example

The following example configures dot1x re-authentication period to 7200s:

```
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 is from 1 to 65535s.

Default

30s

Usage Guidelines

This command specifies the time interval of the host client to respond to the authentication request. The switch will resend the authentication request when exceeding this time interval.

Command Mode

Global Configuration Mode

Example

The following command sets 24 as the timeout period:

```
Switch(config)# dot1x timeout tx-period 24
Switch(config)#
```

1.1.11 dot1x mab

Syntax

dot1x mab

no dot1x mab

Parameter

None

Default

Disabled

Usage Guidelines

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 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 multi-auth mode cannot coexist with guest vlan or mab.

Command Mode

Interface Configuration Mode

Example

The following example shows how to enable mab authentication in interface g0/0/1.

```
Switch(config-g0/0/1)# dot1x mab
Switch(config-g0/0/1)#
```

1.1.12 dot1x mabformat

Syntax

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

no dot1x mabformat

Parameter

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

6	MAC address format: AA-BB-CC-DD-EE-FF

Default

The default is 1.

Usage Guidelines

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 configure the mac format as 3.

```
Switch(config)# dot1x mabformat 3
Switch(config)#
```

1.1.13 dot1x user-permit

Syntax

dot1x user-permit xxx

no dot1x user-permit

Parameter

Parameter	**Syntax**
xxx	Username

Default

All users are allowed to pass without user-bind.

Usage Guidelines

Use this command to bind user on the interface, one user can be binded on each interface. When enabled 802.1x authentication, the authentication is only available to the binding user.

Command Mode

Interface configuration mode

Example

The following example configures a as the binding user on interface g0/0/1:

```
Switch(config-g0/0/1)# dot1x user-permit a
Switch(config-g0/0/1)#
```

1.1.14 dot1x guest-vlan

Syntax

Enable the guest-vlan feature of the dot1x with **dot1x guest-vlan** command in global configuration mode, and disable with the no form of this command.

dot1x guest-vlan

no dot1x guest-vlan

Parameter

None

Default

Disable

Usage Guidelines

When you enable the guest-vlan command, the software will assign the corresponding port to a guest VLAN when it does not receive a response from the client.

This command is used with the **dot 1x guest-valan id** interface configuration command.

Note: This command cannot be configured with **multiple-auth** command simultaneously.

Command Mode

Global configuration mode

Example

The following example enables guest-vlan feature in global configuration mode:

```
Switch(config)#dot1x guest-vlan
```

1.1.15 dot1x guest-vlan id

Syntax

To configure dot1x guest-vlan id value (range from 1 to 4094) on an interface, use the **dot1x guest-vlan** command. Use the no form of this command to restore the default value.

dot1x guest-vlan id

no dot1x guest-vlan

Parameter

Id: guest vlan value, which can be any configured vlan id in the system.

Default

None

Usage Guidelines

When you enable the guest-vlan command, the software will assign the corresponding port to a guest VLAN when it does not receive a response from the client.

This command is used with the **dot1x guest-vlan** global configuration command.

Note: This command cannot be configured with **multiple-auth** command simultaneously.

Command Mode

Interface configuration mode

Example

The following example configures guest-vlan id value on the interface g0/0/1:

```
Switch(config-g0/0/1)#dot1x guest-vlan 2
```

1.1.16 dot1x forbid multi-network-adapter

Syntax

To forbid the supplicant of the multi-network-adapter, use the **dot1x forbid multi-network-adapter** command. Use no form of this command to restore the default configuration.

dot1x forbid multi-network-adapter

no dot1x forbid multi-network-adapter

Parameter

None

Default

None

Usage Guidelines

Use this command to forbid the supplicant of the multi-network-adapter to avoid occurrence of the agent.

Command Mode

Interface configuration mode

Example

The following example forbids the supplicant of the multi-network-adapter on the interface g0/0/1:

```
Switch(config-g0/0/1)# dot1x forbid multi-network-adapter
```

1.1.17 dot1x keepalive

Syntax

dot1x keepalive

no dot1x keepalive

To enable/disable the keepalive detection for the authentication user in the global configuration mode, run the above commands.

Parameter

None

Default

Enable

Usage Guidelines

The default is to enable the keepalive detection.

Command Mode

Global configuration mode

Example

The following example shows how to disable the keepalive function.

```
Switch(config)#no dot1x keepalive
Switch(config)#
```

1.1.18 aaa authentication dot1x

Syntax

aaa authentication dot1x default *method*

no aaa authentication dot1x default

Parameter

Parameter	Syntax
method	radius, local

Default

None

Usage Guidelines

The method parameter identifies the list of methods that the authentication algorithm tries in the given sequence to validate the password provided by the client. It is best to use radius authentication for the 802.1X aaa authentication, or you can use local configuration data for authentication, such as the user password stored locally in the configuration.

Command Mode

Global configuration mode

Example

The following example configures RADIUS as the dot1x authentication method:

```
Switch(config)#aaa authentication dot1x default radius
Switch(config)#
```

1.1.19 debug dot1x errors

Syntax

debug dot1x errors

Parameter

None

Default

None

Usage Guidelines

This command is used to debug all error information during dot1x running to locate errors.

1.1.20 debug dot1x state

Syntax

debug dot1x state

Parameter

None

Default

None

Usage Guidelines

Output format is as follows:

```
2003-3-18 17:40:09 802.1x:AuthSM(g0/0/1) state Connecting-> Authenticating, event rxRespId
2003-3-18 17:40:09 802.1x:g0/0/1 Create user for Enter authentication
2003-3-18 17:40:09 802.1x:BauthSM(g0/0/1) state Idle-> Response, event authStart
2003-3-18 17:40:09 802.1x:g0/0/1 user "myname" denied, Authentication Force Failed
2003-3-18 17:40:09 802.1x:g0/0/1 Authentication Fail
2003-3-18 17:40:09 802.1x:BauthSM(g0/0/1) state Response-> Fail, event aFail
```

1.1.21 debug dot1x packet

Syntax

debug dot1x packet

Parameter

None

Default

None

Usage Guidelines

```
2003-3-18 17:40:09 802.1x:g0/0/1 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:g0/0/1 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
```

1.1.22 show dot1x

Syntax

To show 802.1x configuration information, use the **show dot1x** command.

show dot1x [**interface** *intf-id* | **statistics**/**run-config** [**interface** *intf-id*]/**debug**]

Parameter

Parameter	Description
interface	Shows the dot1x interface information
intf-id	The concrete physical interface.
statistics	Shows the dot1x statistics information
run-config	Shows the dot1x configuration information
debug	Shows the debug information

Default

None

Usage Guidelines

This command is used to show 802.1x configuration information.

Command Mode

EXEC or configuration mode

Example

The following example shows how to display 802.1x configuration information:

```
Switch_config#show 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 g0/0/1 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
```