

802.1x Configuration Commands (GTL-2091)



V1.0

Digital Data Communications GmbH, Germany.

<http://www.level1.com>

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 multiple-hosts	4
1.1.4 dot1x default	5
1.1.5 dot1x max-req	5
1.1.6 dot1x reauth-max	6
1.1.7 dot1x re-authentication	7
1.1.8 dot1x timeout quiet-period	8
1.1.9 dot1x timeout re-authperiod	9
1.1.10 dot1x timeout tx-period	9
1.1.11 dot1x user-permit	10
1.1.12 dot1x authentication method	11
1.1.13 dot1x accounting enable	12
1.1.14 dot1x accounting method	13
1.1.15 dot1x authen-type、dot1x authentication type	13
1.1.16 dot1x guest-vlan	14
1.1.17 dot1x guest-vlan id	15
1.1.18 dot1x forbid multi-network-adapter	16
1.1.19 aaa authentication dot1x	17
1.1.20 debug dot1x error	18
1.1.21 debug dot1x state	18
1.1.22 debug dot1x packet	19
1.1.23 show dot1x	19

Chapter 1 802.1x Configuration Commands

1.1 802.1x Configuration Commands

802.1x configuration commands include:

- dot1x enable
- dot1x port-control
- dot1x multiple-hosts
- dot1x default
- dot1x max-req
- dot1x reauth-max
- dot1x re-authentication
- dot1x timeout quiet-period
- dot1x timeout re-authperiod
- dot1x timeout tx-period
- dot1x user-permit
- dot1x authentication method
- dot1x authen-type、dot1x authentication type
- dot1x guest-vlan
- dot1x guest-vlan id
- aaa authentication dot1x
- debug dot1x error
- debug dot1x state
- debug dot1x packet
- show dot1x

1.1.1 dot1x enable

Description

dot1x enable

no dot1x enable

Parameter

None

Default

None

Instruction

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

Example

The following example enables dot1x:

```
Console_config#dot1x enable
```

```
Console_config#
```

1.1.2 dot1x port-control

Description

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

no dot1x port-control

Parameter

Parameter	Description
-----------	-------------

auto	Enables 802.1x protocol authentication method
force-authorized	Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required.
force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.

Default

force-authorized

Instruction

The 802.1X protocol is supported on Layer 2 static-access ports. You can use the auto keyword only if the port is not configured as one of these types:

- Trunk port—If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
- EtherChannel port—Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel or on an active port in an EtherChannel, an error appears, and 802.1X is not enabled. If you enable 802.1X on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.
- Switch Port Analyzer (SPAN) destination port—You can enable 802.1X on a port that is a SPAN destination port; however, 802.1X is disabled until the port is removed as a SPAN destination. You can enable 802.1X on a SPAN source port.

Command mode

interface configuration

Example

The following example enables 802.1x on interface f0/24:

```
Console_config_f0/24)# dot1x port-control auto
Console_config_f0/24)#
```

The following example configures interface f0/23 as the vlan trunk port and enables 802.1x:

```
Console_config_f0/23)#switchport mode trunk
Console_config_f0/23)#dot1x port-control auto
802.1x Control Failed, 802.1x cannot cmd on vlanTrunk port(f0/23)
Console_config_f0/23)#
```

1.1.3 dot1x multiple-hosts

Description

To allow multiple hosts (clients) on an 802.1X-authorized switch port that has the dot1x port-control interface configuration command set to auto, use the dot1x multiple-hosts command. To return to the default setting, use the no form of this command.

dot1x multiple-hosts

no dot1x multiple-hosts

Parameter

None

Default

disabled

Instruction

In multi-host mode, only one of the attached hosts has to be successfully authorized for all hosts to be granted network access (the multi-host mode authenticates one client, but after the client is authenticated, traffic is allowed from all other MAC addresses.). If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN [EAPOL] logoff message is received), all attached clients are denied access to the network.

The single-host mode allows only one client per port, that is, one MAC address to authenticate, and all others are blocked.

Command mode

interface configuration

Example

The following example enables multiple-hosts on interface f0/24:

```
Console_config_f0/24)# dot1x multiple-hosts  
Console_config_f0/24)#
```

1.1.4 dot1x default

Description

To reset the global 802.1X authentication parameters to their default values as specified in the latest IEEE 802.1X standard, use the dot1x default command.

dot1x Default

Parameter

None

Default

None

Instruction

To reset the global 802.1X authentication parameters to their default values.

Command mode

Global configuration

Example

The following example shows how to reset the global 802.1X parameters:

```
Console_config#dot1x default
Console_config#
```

1.1.5 dot1x max-req

Description

To set the maximum number of times that a networking device or Ethernet switch network module can send an Extensible Authentication Protocol (EAP) request/identity frame to a client (assuming that a response is not received) before restarting the authentication process, use the dot1x max-req command in interface configuration or global configuration mode. To set the number of times to the default setting of 2, use the no form of this command.

dot1x max-req *count*

no dot1x max-req

Parameter

Parameter	Description
<i>count</i>	Maximum number of retries. The value is from 1 through 10.

Default

2

Instruction

Change the maximum number of retries to ensure to pass the authentication between certain clients and authentication servers.

Command mode

Global configuration

Example

The following example sets 4 as the maximum number of times:

```
Console_config#dot1x max-req 4
```

```
Console_config#
```

1.1.6 dot1x reauth-max**Description**

dot1x reauth-max *count*

no dot1x reauth-max

Parameter

Parameter	Description
<i>count</i>	Maximum number of retries. The value is from 1 through 10.

Default

4

Instruction

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

Command mode

Global configuration

Example

The following example set 5 as the maximum number of reauthentications:

```
Console_config#dot1x reauth-max 5
```

```
Console_config#
```

1.1.7 dot1x re-authentication**Description**

To enable the periodic reauthentication of the client, use the dot1x re-authentication command. To return to the default setting, use the no form of this command.

dot1x re-authentication

no dot1x re-authentication

Parameter

None

Default

None

Instruction

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

Command mode

Global configuration

Example

This example shows how to enable the periodic reauthentication:

```
Console_config#dot1x re-authentication
```

```
Console_config#
```

1.1.8 dot1x timeout quiet-period

Description

dot1x timeout quiet-period *time*

no dot1x timeout quiet-period

Parameter

Parameter	Description
<i>time</i>	Period of reenabling authentication, in the range from 0 to 65535 seconds

Default

60s

Instruction

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

Example

The following example configures quiet period value to 40:

```
Console_config#dot1x timeout quiet-period 40
```

```
Console_config#
```

1.1.9 dot1x timeout re-authperiod

Description

dot1x timeout re-authperiod *time*

no dot1x timeout re-authperiod

Parameter

Parameter	Description
<i>time</i>	Period of reauthentication, in the range from 1 to 4294967295 seconds

Default

3600s

Instruction

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

Command mode

Global configuration

Example

The following example configures dot1x reauthentication period to 7200s:

```
Console_config# dot1x timeout re-authperiod 7200
Console_config#
```

1.1.10 dot1x timeout tx-period

Description

dot1x timeout tx-period *time*

no dot1x timeout tx-period

Parameter

Parameter	Description
time	Time is from 1 to 65535s.

Default

30s

Instruction

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

Example

The following command sets 24 as the timeout period:

```
Console_config_f0/0)# dot1x timeout tx-period 24
```

```
Console_config_f0/0)#
```

1.1.11 dot1x user-permit**Description**

dot1x user-permit xxx yyy zzz

no dot1x user-permit

Parameter

Parameter	Description
xxx	Username
yyy	Username
zzz	Username

Default

All users are allowed to pass without user-bind.

Instruction

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

Command mode

interface configuration

Example

The following example configures a,b,c,d as the binding user on interface f0/1:

```
Console_config_f0/1# dot1x user-permit a b c d
```

```
Console_config_f0/1#
```

1.1.12 dot1x authentication method

Description

dot1x authentication method xxx

no dot1x authentication method

Parameter

Parameter	Description
xxx	Method name

Default

“default” method

Instruction

Use this command to configure authentication method on an interface. This command is one of the authentication methods that AAA provides. Each interface only uses one authentication method. When AAA performs authentication for users of 802.1x, it will select the configured authentication method to perform.

Command mode

interface configuration

Example

The following example configures abcd as the authentication method on interface f0/1; this method uses local username for authentication. The following example configures efgh as the authentication method on interface f0/2:

```
Console_config #aaa authentication dot1x abcd local
Console_config #aaa authentication dot1x efgh radius
Console_config #int f0/1
Console_config_f0/1# dot1x authentication method abcd
Console_config_f0/1# int f0/2
Console_config_f0/2)# dot1x authentication method efgh
```

1.1.13 dot1x accounting enable

Description

dot1x accounting enable

no dot1x accounting enable

Parameter

Parameter	Description
None	

Default

The accounting function is disabled.

Explanation

The accounting function must be used together with the authentication function. You'd better enable the dotx re-authentication function.

Command mode

Port configuration mode

Example

The following commands are used to configure the dot1x authentication function on port f0/1 and enable the accounting function:

```
Console_config #dot1x enable
Console_config #int f0/1
Console_config_f0/1# dot1x port atuo
```

```
Console_config_f0/1# dot1x accounting enable
```

1.1.14 dot1x accounting method

Description

dot1x accounting method xxx

no dot1x accounting method

Parameter

Parameter	Description
xxx	Name of the accounting method

Default

the **default** method

Explanation

The accounting method configured by this command must be one of the AAA accounting methods. Each port has only one accounting method. After the dot1x accounting function is enabled, the method is used for accounting.

Command mode

Port configuration mode

Example

In the following example, an **abcd** accounting method is set for port f0/1. The radius server must be used in this method.

```
Console_config # aaa accounting network abcd start-stop group radius
```

```
Console_config #radius host 192.168.20.100
```

```
Console_config #int f0/1
```

```
Console_config_f0/1# dot1x accounting method abcd
```

1.1.15 dot1x authen-type、 dot1x authentication type

Description

To configure global dot1x authentication type, use the **dot1x authen-type command**.
Use the no form of this command to restore the default value.

dot1x authen-type {chap|eap}

no dot1x authen-type

Parameter

None

Default

Default global is chap.

Default on an interface refers to the default global.

Instruction

Use this command to configure authentication type. The authentication type will decide AAA to use Chap or Eap. The challenge that MD5 needs will be formed locally when using Chap. The challenge that MD5 needs will be formed on the authentication server when using Eap. Each interface only uses one kind of authentication type. It is the globally-configured one by default. The interface will not stop using this kind of authentication type until the no form of this command is used.

Command mode

Interface and global configuration

Example

The following example configures Chap and Eap as the authentication type and the global authentication type on the interface f0/1

```
Console_config #dot1x authen-type eap
```

```
Console_config #int f0/1
```

```
Console_config_f0/1# dot1x authentication type chap
```

1.1.16 dot1x guest-vlan

Description

To specify an active VLAN as an IEEE 802.1x guest VLAN, use the dot1x guest-vlan command in interface configuration mode. To return to the default setting, use the no form of this command.

dot1x guest-vlan

no dot1x guest-vlan

Parameter

None

Default

No guest VLAN is configured.

Instruction

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-vlan id interface configuration command.

Command mode

Global configuration

Example

The following example enables global guest-vlan feature:

Console_config #dot1x guest-vlan

1.1.17 dot1x guest-vlan id**Description**

To configure dot1x guest-vlan id value 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

0

Instruction

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-vlan global configuration command.

Command mode

interface configuration

Example

The following example configures guest-vlan id value on an interface:

Console_config_if) #dot1x guest-vlan 2

1.1.18 dot1x forbid multi-network-adapter**Description**

dot1x forbid multi-network-adapter

no dot1x forbid multi-network-adapter

Run **dot1x forbid multi-network-adapter** to configure the Supplicant to shut down multiple network adapters. Run **no dot1x forbid multi-network-adapter** to resume the default configuration.

Parameter

None

Default

None

Explanation

This command can disable the Supplicant with multiple network adapters to prevent the agent.

Command mode

Port configuration mode

Example

The following command is run in port mode to disable the Supplicant with multiple network adapters.

```
Console_config_if) # dot1x forbid multi-network-adapter
```

1.1.19 aaa authentication dot1x

Description

To specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X, use the `aaa authentication dot1x` command. To disable authentication, use the `no` form of this command

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

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

Parameter

Parameter	Description
Default	Uses the listed authentication methods that follow this parameter as the default list of methods when a user logs in.
<i>method1</i> [<i>method2...</i>]	enable 、 group radius、 line、 local、 local-case、 None

Default

No authentication is performed.

Instruction

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. The only method that is truly 802.1X-compliant is the group radius method, in which the client data is validated against a RADIUS authentication server. The remaining methods enable AAA to authenticate the client by using locally configured data. For example, the local and local-case methods use the username and password that are saved in the configuration file. The enable and line methods use the enable and line passwords for authentication.

Command mode

Global configuration

Example

The following example configures RADIUS as the dot1x authentication method:

```
Console_config#aaa authentication dot1x default radius
```

```
Console_config#
```

1.1.20 debug dot1x error

Description

debug dot1x error

Parameter

None

Default

None

Instruction

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

1.1.21 debug dot1x state

Description

debug dot1x state

Parameter

None

Default

None

Instruction

Output format is as follows:

```
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

1.1.22 debug dot1x packet

Description

debug dot1x packet

Parameter

None

Default

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

1.1.23 show dot1x

Description

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

show dot1x [interface *intf-id*]

Parameter

Parameter	Description
<i>intf-id</i>	The concrete physical interface.

Default

None

Instruction

This command is used to show 802.1x configuration information.

Command mode

EXEC

Example

The following example configures dot1x port-control auto on the interface f0/10:

```
Console_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
```

