

## 802.1x配置命令

---

# 目 录

第 1 章 802.1x 配置命令.....	1
1.1 802.1x 配置命令.....	1
1.1.1 dot1x enable.....	2
1.1.2 dot1x port-control.....	3
1.1.3 dot1x authentication multiple-hosts.....	4
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.....	12
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 dot1x keepalive.....	18
1.1.22 dot1x vendor-permit.....	19
1.1.23 dot1x vendor.....	20
1.1.24 aaa authentication dot1x.....	21
1.1.25 debug dot1x errors.....	22
1.1.26 debug dot1x state.....	22
1.1.27 debug dot1x packet.....	23
1.1.28 show dot1x.....	23

## 第 1 章 802.1x 配置命令

### 1.1 802.1x配置命令

802.1x 的配置命令有:

- 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 accounting enable
- dot1x accounting method
- dot1x authen-type、dot1x authentication type
- dot1x guest-vlan
- dot1x guest-vlan id
- dot1x forbid multi-network-adapter
- dot1x keepalive
- Dot1x vendor-permit
- Dot1x vendor

- aaa authentication dot1x
- debug dot1x error
- debug dot1x state
- debug dot1x packet
- show dot1x

### 1.1.1 dot1x enable

#### 命令描述

**dot1x enable**

**no dot1x enable**

#### 参数

无

#### 缺省

无

#### 使用说明

使能 802.1x 功能，如果没有使能 802.1x 功能，则在端口下是不能启动 802.1x 功能的，如果禁止 802.1x 功能，则所有 802.1x 功能的端口将取消掉 802.1x 功能，同时，所有的 802.1x 报文将不会被 CPU 接收，而会像一般的组播报文一样在 VLAN 内转发。

#### 命令模式

全局配置模式

#### 示例

下面的命令将启动 dot1x。

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

## 1.1.2 dot1x port-control

### 命令描述

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

**no dot1x port-control**

### 参数

参数	参数说明
<b>auto</b>	启用802.1x协议认证方式。
<b>force-authorized</b>	强制端口认证通过。
<b>force-unauthorized</b>	强制端口认证不通过。

### 缺省

force-authorized

### 使用说明

802.1x 协议是一种两层的基于端口的认证方式，使用 **auto** 命令可以启动该认证方式，该认证方式只能配置于物理端口，且该端口属性不能是 **vlan** 主干、动态存取、安全端口、监控端口。

### 命令模式

接口配置模式

### 示例

下面的命令将在 **g0/1** 上启动 **802.1x**。

```
Switch_config_g0/1# dot1x port-control auto
Switch_config_g0/1#
```

下面的命令先将 **g0/1** 配置为 **vlan** 主干，然后启动 **802.1x**。

```
Switch_config_g0/1#switchport mode trunk
Switch_config_g0/1#dot1x port-control auto
802.1x Control Failed, 802.1x cannot cmd on vlanTrunk port(g0/1)
Switch_config_g0/1#
```

### 1.1.3 dot1x authentication multiple-hosts

#### 命令描述

**dot1x authentication multiple-hosts**

**no dot1x authentication multiple-hosts**

#### 参数

无

#### 缺省

禁止 802.1x 的多用户访问。

#### 使用说明

将一个端口配置为 802.1x 的 multi-hosts 访问模式后，交换机将对不同的用户进行认证，当某一用户认证通过后，则将端口置为 up 状态。此时，其它用户无需认证也可以通过该端口进行访问。

**注意：**修改多主机认证模式后，需要对端口下所有用户进行重新认证。

#### 命令模式

端口配置模式

#### 示例

下面的命令将在 g0/1 上启动 multiple-hosts 认证。

```
Switch_config_g0/1# dot1x authentication multiple-hosts
```

```
Switch_config_g0/1#
```

### 1.1.4 dot1x authentication multiple-auth

#### 命令描述

**dot1x authentication multiple-auth**

**no dot1x authentication multiple-auth**

## 参数

无

## 缺省

禁止 802.1x 的多用户认证。

## 使用说明

将一个端口配置为 802.1x 的 **mutiple-auth** 认证模式后，交换机将对每个用户分别进行认证，不同用户认证之间互不影响。只要有一个用户认证成功，端口就 **up**，只有当所有的用户都认证失败，即认证端口下不存在认证成功的用户时，端口才 **down**。这样可以保证对每个用户分别认证，且一个用户认证失败不影响其他用户的正常访问权限。

**注意：** **multi-auth** 认证模式与 **guest vlan** 不能同时配置，与 **mab** 也不能同时配置。修改多主机认证模式，需要对端口下所有用户进行重新认证。

## 命令模式

端口配置模式

## 示例

下面的命令将在 **g0/1** 上启动 **mutiple-auth** 认证。

```
Switch_config_g0/1# dot1x authentication multiple-auth  
Switch_config_g0/1#
```

### 1.1.5 dot1x default

#### 命令描述

**dot1x default**

#### 参数

无

#### 缺省

无

## 使用说明

将所有的全局配置恢复到默认配置。

## 命令模式

全局配置模式

## 示例

下面的命令将 **dot1x** 所有的配置参数恢复到默认值。

```
Switch_config #dot1x default
Switch_config #
```

### 1.1.6 dot1x reauth-max

## 命令描述

**dot1x reauth-max** *count*

**no dot1x reauth-max**

## 参数

参数	参数说明
<i>count</i>	认证重试的最大次数，范围1-10。

## 缺省

5

## 使用说明

设置重复认证的次数，超过该次数的认证，客户机没有响应，认证将会被挂起。

## 命令模式

全局配置模式

## 示例

下面的命令将配置 **dot1x** 身份认证请求的最大次数为 **4**。



```
Switch_config #dot1x reauth-max 4
Switch_config #
```

### 1.1.7 dot1x re-authentication

#### 命令描述

```
dot1x re-authentication
no dot1x re-authentication
```

#### 参数

无

#### 缺省

无

#### 使用说明

启动重认证功能，当端口认证通过以后，还会周期性的向主机进行认证，该周期可以通过命令 `dot1x timeout re-authperiod`，进行配置。

#### 命令模式

全局配置模式

#### 示例

下面的命令将启动重认证功能。

```
Switch_config #dot1x re-authentication
Switch_config #
```

### 1.1.8 dot1x timeout quiet-period

#### 命令描述

```
dot1x timeout quiet-period time
no dot1x timeout quiet-period
```

## 参数

参数	参数说明
<i>time</i>	dot1x重启认证的周期，范围0-65535s。

## 缺省

60s

## 使用说明

在认证失败后有一段安静时间，在该时间内，交换机将不会接受或启动任何认证。

## 命令模式

全局配置模式

## 示例

下面的命令将配置 `quiet-period` 的值为 40。

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

## 1.1.9 dot1x timeout re-authperiod

## 命令描述

**dot1x timeout re-authperiod *time***

**no dot1x timeout re-authperiod**

## 参数

参数	参数说明
<i>time</i>	dot1x重认证的周期值，1-4294967295s。

## 缺省

3600s

## 使用说明

该命令只有在启动重认证后才会产生作用。

## 命令模式

全局配置模式

## 示例

下面的命令将配置 dot1x 重认证的周期为 7200s。

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

```
Switch_config #
```

### 1.1.10 dot1x timeout tx-period

## 命令描述

**dot1x timeout tx-period *time***

**no dot1x timeout tx-period**

## 参数

参数	参数说明
time	时间，1- 65535s。

## 缺省

30s

## 使用说明

该命令可以配置主机客户端响应认证请求的时间间隔，超过该时间交换机将重发认证请求。

## 命令模式

全局配置模式

## 示例

下面的命令将配置发送频率为 24。

```
Switch_config # dot1x timeout tx-period 24
```

```
Switch_config #
```

## 1.1.11 dot1x mab

### 命令描述

**dot1x mab**

**no dot1x mab**

### 参数

无

### 缺省

关闭

### 使用说明

当对端设备无法使用 802.1x 客户端软件时,交换机使用 Mab(MAC Authentication Bypass) 认证方式,将对端设备的 mac 地址作为用户名和密码发往 radius 服务器进行认证。

开启 mab 认证后,如果对端设备既没有发送 eapol\_start 报文,也没有响应 request\_identity 报文,超时后,交换机认为对端设备不支持 802.1x 认证客户端,转而进入 mab 认证过程。交换机将获取到的设备的 mac 地址作为用户名和密码发送给 radius 服务器进行认证,如果在 radius 服务器上已经授权该 mac 地址,则认证成功,允许用户通过该端口访问网络。

**注意:** 开启 mab 认证时,不能同时配置 multi-auth 多主机认证模式。

### 命令模式

端口配置模式

### 示例

下面的命令将在 g0/1 端口启动 mab 认证。

```
Switch_config_g0/1# dot1x mab
Switch_config_g0/1#
```

## 1.1.12 dot1x mabformat

### 命令描述

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

**no dot1x mabformat**

### 参数

参数	参数说明
1	MAC地址格式: aa:bb:cc:dd:ee:ff
2	MAC地址格式: AA:BB:CC:DD:EE:FF
3	MAC地址格式: aabbccddeeff
4	MAC地址格式: AABCCDDEEFF
5	MAC地址格式: aa-bb-cc-dd-ee-ff
6	MAC地址格式: AA-BB-CC-DD-EE-FF

### 缺省

默认为 1

### 使用说明

当开启 mab 认证时，可以通过该命令设置交换机发送给 radius 服务器的 mac 地址格式。

### 命令模式

全局配置模式

### 示例

下面的命令将配置 mac 格式为 3。

```
Switch_config # dot1x mabformat 3
Switch_config #
```

### 1.1.13 dot1x user-permit

#### 命令描述

**dot1x user-permit xxx yyy zzz**

**no dot1x user-permit**

#### 参数

参数	参数说明
xxx	用户名。
yyy	用户名。
zzz	用户名。

#### 缺省

没有用户绑定，所有用户都通过。

#### 使用说明

该命令配置端口下绑定的用户，每一个端口下可以绑定 8 个用户；当启动 802.1x 认证时，只会对绑定的用户名执行认证，其他用户不执行认证，肯定认证失败。

#### 命令模式

端口配置模式

#### 示例

下面的命令将 g0/1 配置绑定用户为 a、b、c、d。

```
Switch_config_g0/1# dot1x user-permit a b c d
```

```
Switch_config_g0/1#
```

### 1.1.14 dot1x authentication method

#### 命令描述

**dot1x authentication method xxx**

**no dot1x authentication method**

## 参数

参数	参数说明
xxx	方法名。

## 缺省

“default”方法。

## 使用说明

该命令配置端口下的认证方法，该方法应是 AAA 中提供的认证方法之一，每一个端口只使用一种方法；当 AAA 对 802.1x 的用户进行认证时，AAA 将会选择配置的认证方法执行认证。

## 命令模式

端口配置模式

## 示例

下面的命令将在端口 g0/1 配置认证方法为 abcd，该方法使用本地用户名认证；在端口 g0/2 配置认证方法为 efgh，该方法使用 radius 远程认证。

```
Switch_config #aaa authentication dot1x abcd local
Switch_config #aaa authentication dot1x efgh group radius
Switch_config #int g0/1
Switch_config _g0/1# dot1x authentication method abcd
Switch_config _g0/1# int g0/2
Switch_config _g0/2# dot1x authentication method efgh
```

### 1.1.15 dot1x accounting enable

#### 命令描述

**dot1x accounting enable**  
**no dot1x accounting enable**

#### 参数

无

## 缺省

关闭记帐功能。

## 使用说明

该命令打开端口下的记帐功能，必须和认证功能结合。最好开启 **dot1x** 重认证功能使用。

## 命令模式

端口配置模式

## 示例

下面的命令将在端口 **g0/1** 配置 **dot1x** 认证并打开记帐功能。

```
Switch_config #dot1x enable
Switch_config #int g0/1
Switch_config _g0/1# dot1x port auto
Switch_config _g0/1# dot1x accounting enable
```

### 1.1.16 dot1x accounting method

## 命令描述

**dot1x accounting method xxx**

**no dot1x accounting method**

## 参数

参数	参数说明
xxx	记帐方法名

## 缺省

“default”方法。

## 使用说明

该命令配置端口下的记帐方法，该方法应是 **AAA** 中提供的记帐方法之一，每一个端口只使用一种方法；当打开 **dot1x** 记帐功能后，将使用该方法进行记帐。



## 命令模式

端口配置模式

## 示例

下面的命令将在端口 `g0/1` 配置记帐方法为 `abcd`，该方法使用 `radius` 服务器；并在端口 `g0/1` 下配置记帐方法为 `abcd`。

```
Switch_config # aaa accounting network abcd start-stop group radius
Switch_config #radius host 192.168.20.100
Switch_config #int g0/1
Switch_config _g0/1# dot1x accounting method abcd
```

### 1.1.17 dot1x authen-type、dot1x authentication type

#### 命令描述

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

**no dot1x authen-type**

配置全局下 `dot1x` 的认证类型，`no` 命令恢复为默认值。

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

**no dot1x authentication type**

配置端口下 `dot1x` 的认证类型，`no` 命令恢复为默认值。

#### 参数

无

#### 缺省

全局下默认为 `eap`

端口下默认为全局下的配置类型。

#### 使用说明

该命令配置认证类型，该类型将决定 AAA 使用 `Chap` 或 `Eap` 认证；使用 `Chap` 时 MD5 所需的 `challenge` 将在本地产生，而使用 `Eap` 时 `challenge` 将在认证服务器上产生；每一个端口只使用一种认证类型，默认情况下该类型使用全局配置的认证类型，当端口配置了认证类型时就一直使用该认证类型，除非使用 `No` 命令恢复到默认值。

## 命令模式

端口和全局配置模式

## 示例

下面的命令将在端口 g0/1 配置认证类型为 Chap，全局认证类型为 Eap。

```
Switch_config #dot1x authen-type eap
Switch_config #int g0/1
Switch_config _g0/1# dot1x authentication type chap
```

### 1.1.18 dot1x guest-vlan

#### 命令描述

**dot1x guest-vlan**

**no dot1x guest-vlan**

打开全局下 dot1x 的 guest-vlan 功能，no 命令关闭。

#### 参数

无

#### 缺省

关闭

#### 使用说明

打开 guest-vlan 功能，可以在客户端没有响应时，通过将相应端口划入 guest-vlan，给予特定的网络访问权限。

该命令和端口下配置命令 dot1x guest-vlan id 结合使用。

**注意：**不能与 multiple-auth 命令同时配置。

## 命令模式

全局配置模式

## 示例

下面的命令将在全局模式下打开 `guest-vlan` 功能

```
Switch_config #dot1x guest-vlan
```

### 1.1.19 dot1x guest-vlan id

#### 命令描述

**dot1x guest-vlan id**

**no dot1x guest-vlan**

配置端口的 `dot1x guest-vlan id` 值，`no` 命令恢复默认值为 0。

#### 参数

Id: `guest-vlan` 值，可以是系统内已配置的任何 `vlan id`。

#### 缺省

无

#### 使用说明

打开 `guest-vlan` 功能，可以在客户端没有响应时，通过将相应端口划入 `guest-vlan`，给予特定的网络访问权限。

该命令和全局下配置命令 `dot1x guest-vlan` 结合使用。

**注意：** 不能与 `multiple-auth` 命令同时配置。

#### 命令模式

端口配置模式

#### 示例

下面的命令将在端口 `g0/1` 上配置 `guest-vlan id` 值。

```
Switch_config _g0/1#dot1x guest-vlan 2
```

## 1.1.20 dot1x forbid multi-network-adapter

### 命令描述

**dot1x forbid multi-network-adapter**

**no dot1x forbid multi-network-adapter**

配置端口的禁止多网卡的 Supplicant，no 命令恢复默认配置。

### 参数

无

### 缺省

无

### 使用说明

本命令可以禁止拥有多张网络适配器的 Supplicant 端，防止代理的发生。

### 命令模式

端口配置模式

### 示例

下面的命令将在端口 g0/1 下禁止拥有多张网络适配器的 Supplicant。

```
Switch_config_g0/1 # dot1x forbid multi-network-adapter
```

## 1.1.21 dot1x keepalive

### 命令描述

**dot1x keepalive**

**no dot1x keepalive**

全局配置下，开启、关闭对认证客户端进行存活检测的功能

### 参数

无

### 缺省

开启

### 使用说明

配置交换机对认证客户端进行存活检测，默认开启。

### 命令模式

全局配置模式

### 示例

下面的命令将关闭交换机对认证客户端进行存活检测的功能。

```
Switch_config #no dot1x keepalive  
Switch_config #
```

## 1.1.22 dot1x vendor-permit

### 命令描述

**dot1x vendor-permit**

**no dot1x vendor-permit**

全局模式下，配置开启、关闭 vendor 转发功能。

### 参数

无

### 缺省

关闭

## 使用说明

该命令开启 **vendor** 转发功能，开启后允许交换机在认证过程中向 radius 认证服务器转发 vendor 信息。默认关闭此功能。

该命令与配置命令 **dot1x vendor** 配置使用。

## 命令模式

全局配置模式

## 示例

下面的命令将在全局模式下开启 **vendor** 转发功能

```
Switch_config #dot1x vendor-permit
```

### 1.1.23 dot1x vendor

## 命令描述

**dot1x vendor word**

**no dot1x vendor**

配置向 radius 服务器提交的 vendor 信息。

## 参数

参数	参数说明
<i>word</i>	Vendor信息

## 缺省

无

## 使用说明

配置 vendor 信息。

## 命令模式

全局配置模式

## 示例

下面的命令将在全局模式下配置 **vendor** 名称为 **LENOVO**

```
Switch_config #dot1x vendor LENOVO
```

### 1.1.24 aaa authentication dot1x

#### 命令描述

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

**no aaa authentication dot1x** { *default* | *word* }

#### 参数

参数	参数说明
<i>default</i>	默认认证方法。当没有使用 <code>dot1x authentication method</code> 命令指定认证方法时，使用此认证方式。
<i>word</i>	指定认证方法名称
<i>method1</i> [ <i>method2...</i> ]	group radius、local、local-case、none

#### 缺省

无

#### 使用说明

**method** 参数提供一系列的方法对客户主机提供的密码进行认证，对 802.1x 的 **aaa** 认证方式最好采用 **radius** 认证，也可以使用本地配置数据进行认证，如本地保存于配置中的用户密码。

#### 命令模式

全局配置模式

#### 示例

下面的命令将配置 **dot1x** 认证方式为 **RADIUS**。

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

### 1.1.25 debug dot1x errors

#### 命令描述

**debug dot1x errors**

#### 参数

无

#### 缺省

无

#### 使用说明

用来输出在 dot1x 运行中出现的一切错误信息，用于错误的定位。

### 1.1.26 debug dot1x state

#### 命令描述

**debug dot1x state**

#### 参数

无

#### 缺省

无

#### 使用说明

输出格式如下：

```
2003-3-18 17:40:09 802.1x:AuthSM(G0/1) state Connecting-> Authenticating, event rxRespld
```

```
2003-3-18 17:40:09 802.1x:G0/1 Create user for Enter authentication
```

```
2003-3-18 17:40:09 802.1x:BauthSM(G0/1) state Idle-> Response, event authStart
```

```
2003-3-18 17:40:09 802.1x:G0/1 user "myname" denied, Authentication Force Failed
```

```
2003-3-18 17:40:09 802.1x:G0/1 Authentication Fail
```

```
2003-3-18 17:40:09 802.1x:BauthSM(G0/1) state Response-> Fail, event aFail
```



### 1.1.27 debug dot1x packet

#### 命令描述

**debug dot1x packet**

#### 参数

无

#### 缺省

无

#### 使用说明

```
2003-3-18 17:40:09 802.1xG0/1 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:G0/1 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
```

### 1.1.28 show dot1x

#### 命令描述

**show dot1x [interface *intf-id* | *statistics*]**

这条命令用来显示 802.1x 配置信息。

#### 参数

参数	参数说明
interface	显示dot1x端口信息
<i>intf-id</i>	具体的物理端口。
<i>statistics</i>	显示dot1x统计信息

#### 缺省

无

## 使用说明

显示 802.1x 配置信息。

## 命令模式

管理模式、配置模式

## 示例

下面的命令将显示 802.1x 配置信息。

```
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 G0/1 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
```