```
Switch(config)#radius deadtime 1
Switch(config)#radius dead-criteria time 15 tries 3
Switch(config)#interface f3/1
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#authentication port-control auto
Switch(config-if)#authentication event server dead action authorize vlan 17
Switch(config-if)#end
Switch#show dot1x int fastethernet 3/1 details

Dot1x Info for FastEthernet3/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Critical-Auth             = Enabled
Critical Recovery Action  = Reinitialize
Critical-Auth VLAN        = 17
Dot1x Authenticator Client List
-------------------------------
Supplicant                = 0000.0000.0001
Auth SM State             = AUTHENTICATING
Auth BEND SM Stat         = RESPONSE
Port Status               = AUTHORIZED
Authentication Method     = Dot1x
Authorized By             = Critical-Auth
Operational HostMode      = SINGLE_HOST
Vlan Policy               = 17

Switch#
```

在 Cisco IOS 12.2(46)SG 及以前版本中的配置：

```
Switch#configure terminal
Switch(config)#aaa new-model
Switch(config)#aaa authentication dot1x default group radius
Switch(config)#dot1x system-auth-control
Switch(config)#radius-server host 10.1.2.3 auth-port 1645 acct-port 1646 test username
randomuser idle-time 1 key mykey
Switch(config)#radius deadtime 1
Switch(config)#radius dead-criteria time 15 tries 3
Switch(config)#interface f3/1
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#dot1x port-control auto
Switch(config-if)#dot1x critical
Switch(config-if)#dot1x critical vlan 17
Switch(config-if)#dot1x critical recovery action reinitialize
Switch(config-if)#end
```

```
Switch#show dot1x int fastethernet 3/1 details

Dot1x Info for FastEthernet3/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Critical-Auth             = Enabled
Critical Recovery Action  = Reinitialize
Critical-Auth VLAN        = 17
Dot1x Authenticator Client List
-------------------------------
Supplicant                = 0000.0000.0001
Auth SM State             = AUTHENTICATING
Auth BEND SM Stat         = RESPONSE
Port Status               = AUTHORIZED
Authentication Method     = Dot1x
Authorized By             = Critical-Auth
Operational HostMode      = SINGLE_HOST
Vlan Policy               = 17

Switch#
```

23.2.10 启用后退认证

在配置为多认证模式的 IEEE 802.1x 端口上，可以同时配置 MAB 和（或）Web 认证作为后退认证（Fallback Authentication）方式，用于对不支持 IEEE 802.1x 的主机进行认证。可以通过配置一个认证方法列表来规定选择使用这些不同认证方法的顺序和优先级。有关 MAB 认证的配置方法参见本章前面 23.2.9 节介绍。

启用后退认证的配置步骤如表 23-12 所示。

表 23-12 后退认证的配置步骤

步骤	命令	说明
1	**ip admission name** *rule-name* **proxy http** 例如：Switch(config)#**ip admission name** rule-fallback **proxy http**	配置基于 Web 认证的认证规则
2	**fallback profile** *profile-name* 例如：Switch(config)#**fallback profile** profile- fallback	为基于 Web 认证创建一个后退配置文件，进入后退配置文件配置模式
3	**ip access-group** *rule-name* **in** 例如：Switch(config-fallback-profile)#**ip access-group** acl1 **in**	指定在进行基于 Web 认证前应用一个基于 Web 认证的认证规则，它是需要事先通过 ACL 配置的
4	**ip admission name** *rule-name* 例如：Switch(config-fallback-profile)#**ip admission name** rule-fallback	把以上认证规则与配置文件进行关联，使客户端在进行基于 Web 认证时采用此认证规则进行管理
5	**exit** 例如：Switch(config-fallback-profile)#**exit**	返回全局配置模式

续表

步骤	命令	说明
6	**interface** *type slot/port* 例如：Switch(config)#**interface** gigabitethernet 1/1	键入要配置后退认证的端口，进入接口配置模式
7	Cisco IOS 12.2(50)SG 及以后版本： **authentication port-control auto** 例如：Switch(config-if)#**authentication port-control auto** Cisco IOS Release 12.2(46)SG 及以前版本： **dot1x port-control auto** 例如：Switch(config-if)#**dot1x port-control auto**	在以上端口上启用 IEEE 802.1x 认证
8	**authentication order** *method1* [*method2*] [*method3*] 例如：Switch(config-if)#**authentication order dot1x webauth**	（可选）指后退认证方法列表，可选的认证方法包括 **dot1x**、**mab** 和 **webauth**，它们在列表中的顺序也决定了它们选择使用的优先级，越在前面的优先级越高
9	**authentication priority** *method1* [*method2*] [*method3*] 例如：Switch(config-if)#**authentication priority dot1x mab webauth**	（可选）覆盖上一步根据在认证方法列表中的位置所确定的认证方法优先级设置，通过本命令可以强制设置各个认证方法的优先级，在前面的优先级更高
10	**authentication event fail action next-method** 例如：Switch(config-if)#**authentication event fail action next-method**	指定采用当前认证方法认证失败后自动采用下一个认证方法
11	Cisco IOS 12.2(50)SG 及以后版本： **mab [eap]** 例如：Switch(config-if)#**mab [eap]** Cisco IOS Release 12.2(46)SG 及以前版本： **dot1x mac-auth-bypass [eap]** 例如：Switch(config-if)#**dot1x mac-auth-bypass eap**	启用 MAB（旁路 MAC 地址认证），使用了可选项后则表示在 RADIUS 认证过程中可以使用 EAP 协议
12	**authentication fallback** *profile-name* 例如：Switch(config-if)#**authentication fallback** profile-fallback	使用第 2 步创建的后退配置文件启用基于 Web 的认证
13	**authentication violation [shutdown | restrict]** 例如：Switch(config-if)#**authentication violation shutdown**	（可选）配置安全违例行为模式，默认为关闭端口模式（**shutdown**），具体参见 23.2.4 节
14	**authentication timer inactivity** {*seconds* | **server**} 例如：Switch(config-if)#**authentication timer inactivity** 600	（可选）指定 MAB 和 IEEE 802.1x 认证非活跃超时计时器，默认是禁止这个计时器的。命令的两个参数和选项说明如下： • *seconds*：指定非活跃计时器周期，取值范围为 1~65535 秒 • **server**：指定从认证服务器获取非活跃超时计时器值
15	**authentication timer restart** *seconds* 例如：Switch(config-if)#**authentication timer restart** 120	（可选）指定重新开始一个认证未授权端口的认证进程周期，取值范围为 1~65535 秒，默认为 60 秒
16	**exit** 例如：Switch(config-if)#**exit**	返回全局配置模式
17	**ip device tracking** 例如：Switch(config)#**ip device tracking**	启用 IP 设备跟踪表（这是基于 Web 认证所需的）
18	**exit** 例如：Switch(config)#**exit**	返回特权模式
19	**show dot1x interface** *type slot/port* 例如：Switch#**show dot1x interface** gigabitethernet 1/1	校验以上配置

以下示例配置 IEEE 802.1x 端口 gigabitethernet5/9 的后退认证方法为 MAB 和基于 Web 认证。后退认证规则名为 rule1，后退认证配置文件名为 fallback1。

在 Cisco IOS 12.2(50)SG 及以后版本中的配置：

```
Switch(config)#ip admission name rule1 proxy http
Switch(config)#fallback profile fallback1
Switch(config-fallback-profile)#ip access-group default-policy in
Switch(config-fallback-profile)#ip admission rule1
Switch(config-fallback-profile)#exit
Switch(config)#interface gigabitethernet5/9
Switch(config-if)#switchport mode access
Switch(config-if)#authentication port-control auto
Switch(config-if)#dot1x pae authenticator
```

```
Switch(config-if)#authentication order dot1x mab webauth
Switch(config-if)#mab eap
Switch(config-if)#authentication fallback fallback1
Switch(config-if)#exit
Switch(config)#ip device tracking
Switch(config)#exit
```

要确定一个配置了后退认证的 IEEE 802.1x 端口上的主机是否经过了认证，可以通过 **show authentication sessions interface** 命令查看当前认证管理器会话信息。示例如下，从输出信息中可以看出，该端口上配置 IEEE 802.1x 和 MAB 两种认证方法，首先采用 IEEE 802.1x 认证方法，且成功认证（注意输出信息中的粗体字部分）：

```
Switch#show authentication sessions interface gigabitethernet5/9
            Interface:  GigabitEthernet5/9
          MAC Address:  0060.b057.4687
           IP Address:  Unknown
            User-Name:  test2
               Status:  Authz Success
               Domain:  DATA
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A8013F0000000901BAB560
     Acct Session ID:  0x0000000B
              Handle:  0xE8000009

Runnable methods list:
      Method     State
      dot1x      Authc Success
      mab        Not run
```

还可使用 **show dot1x interface** 命令查看指定接口上的 IEEE 802.1x 认证配置详细信息。示例如下（注意输出信息中的粗体字部分）：

```
Switch#show dot1x interface gigabitethernet5/9 detail
Dot1x Info for GigabitEthernet5/9
-----------------------------------
PAE                     = AUTHENTICATOR   !---显示端口角色为认证者
PortControl             = AUTO   !---显示客户端的认证状态由交换机检测确定
ControlDirection        = Both   !---显示端口对双方向通信都进行认证
HostMode                = MULTI_AUTH   !---显示端口 IEEE 802.1x 认证模式为多认证模式
QuietPeriod             = 60   !---显示认证失败后再次进行认证所需等待的时间为 60 秒
ServerTimeout           = 0    !---显示交换机在向 RADIUS 服务器发送 EAPOL 认证请求包而没有收到来自 RADIUS 服务器响应时，不再等待就重传请求
SuppTimeout             = 30   !---显示交换机在向客户端发送 EAPOL 标识请求包而没收到来自客户端的响应时，等待 30 秒再重发请求
ReAuthMax               = 2   !---显示最多进行 2 次重认证
MaxReq                  = 2   !---显示交换机最多向客户端发送 2 次 EAPOL 标识请求
TxPeriod                = 2   !---显示交换机向客户端发送 EAPOL 标识请求包中的延时时间为 2 秒
Dot1x Authenticator Client List
-------------------------------
Supplicant              = 0060.b057.4687
Session ID              = C0A8013F0000000901BAB560
    Auth SM State       = AUTHENTICATED
    Auth BEND SM State  = IDLE
Port Status             = AUTHORIZED
```

要显示主机是否使用了 MAB 认证和 MAB 认证配置，可以使用 **show authentication sessions interface** 命令和 **show mab interface** 命令进行查看。示例如下（注意输出信息中的粗体字部分）：

```
Switch#show authentication sessions interface GigabitEthernet7/2
            Interface:  GigabitEthernet7/2
          MAC Address:  0060.b057.4687
           IP Address:  192.168.22.22
            User-Name:  0060b0574687
               Status:  Authz Success
               Domain:  DATA
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
        Vlan Policy:  N/A
    Session timeout:  N/A
       Idle timeout:  N/A
  Common Session ID:  C0A8013F0000000B01BBD278
    Acct Session ID:  0x0000000D
             Handle:  0xF500000B
Runnable methods list:
      Method    State
      dot1x     Failed over
      mab       Authc Success

Switch#show mab interface GigabitEthernet7/2 detail
MAB details for GigabitEthernet7/2
--------------------------------------
Mac-Auth-Bypass              = Enabled

MAB Client List
---------------
Client MAC                   = 0060.b057.4687
Session ID                   = C0A8013F0000000B01BBD278
MAB SM state                 = TERMINATE
Auth Status                  = AUTHORIZED
```

要显示主机是否使用了基于 Web 的认证和 Web 认证配置，可以使用 **show authentication sessions interface** 命令和 **show ip admission cache** 命令进行查看。示例如下（注意输出信息中的粗体字部分）：

```
Switch#show authentication sessions interface G4/3
            Interface:  GigabitEthernet4/3
          MAC Address:  0015.e981.0531
           IP Address:  10.5.63.13
               Status:  Authz Success
               Domain:  DATA
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
        Vlan Policy:  N/A
    Session timeout:  N/A
       Idle timeout:  N/A
  Common Session ID:  0A053F0F0000000200112FFC
    Acct Session ID:  0x00000003
             Handle:  0x09000002
Runnable methods list:
      Method    State
      dot1x     Failed over
      mab       Failed over
      webauth   Authc Success

Switch#show ip admission cache
Authentication Proxy Cache
Total Sessions: 1 Init Sessions: 0
 Client IP 10.5.63.13 Port 4643, timeout 1000, state ESTAB
```

下面是一个在 Cisco IOS 12.2(46)SG 及以前版本中的后退认证配置示例：

```
Switch(config)#ip admission name rule1 proxy http
Switch(config)#fallback profile fallback1
Switch(config-fallback-profile)#ip access-group default-policy in
Switch(config-fallback-profile)#ip admission rule1
Switch(config-fallback-profile)#exit
Switch(config)#interface gigabit5/9
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x port-control auto
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#authentication order dot1x mab webauth
Switch(config-if)#dot1x mac-auth-bypass eap
Switch(config-if)#adot1x fallback fallback1
Switch(config-if)#exit
Switch(config)#ip device tracking
Switch(config)#exit
```

23.2.11 启用周期性重认证

可以启用 IEEE 802.1x 周期性重认证功能，并且指定重认证周期。如果在启用重认证功能前没有指定周期值，则重认证周期为 3600 秒。

自动进行的周期性重认证是基于每个端口进行配置，应用于连接在对应端口上的所有客户端，具体的配置步骤如表 23-13 所示。

表 23-13 周期性重认证配置步骤

步骤	命令	说明
1	**configure terminal** 例如：Switch#**configure terminal**	进入全局配置模式
2	**interface** *interface-id* 例如：Switch(config)#**interface** gigabitethernet 1/1	键入要配置周期性重认证的端口，进入接口配置模式
3	**switchport mode access** 例如：Switch(config-if)#**switchport mode access**	把以上端口转换为二层访问模式
4	**dot1x pae authenticator** 例如：Switch(config-if)#**dot1x pae authenticator**	使用默认参数在以上端口上启用 IEEE 802.1x 认证
5	Cisco IOS 12.2(50)SG 及以后版本： **authentication periodic** 例如：Switch(config-if)#**authentication periodic** Cisco IOS Release 12.2(46)SG 及以前版本： **dot1x reauthentication** 例如：Switch(config-if)#**dot1x reauthentication**	对连接在以上端口上的客户端启用周期性重认证功能，默认是禁止重认证功能，可用 **no authentication periodic** 或 **no dot1x reauthentication** 接口配置模式命令禁止端口上的周期性重认证功能
6	Cisco IOS 12.2(50)SG 及以后版本： **authentication timer reauthenticate** {*seconds* | **server**} 例如：Switch(config-if)#**authentication timer reauthenticate** 1800 Cisco IOS Release 12.2(46)SG 及以前版本： **dot1x timeout reauth-period** {*seconds* | **server**} 例如：Switch(config-if)#**authentication timer reauthenticate server**	手工指定重认证周期，或者从 RADIUS 服务器获得重认证周期值，取值范围为 1~65535 秒，默认为 3600 秒。可用 **no authentication timer reauthenticate** 或 **no dot1x timeout reauth-attempts** 接口配置模式命令恢复为默认设置
7	Cisco IOS 12.2(50)SG 及以后版本： **authentication port-control auto** 例如：Switch(config-if)#**authentication port-control auto** Cisco IOS Release 12.2(46)SG 及以前版本： **dot1x port-control auto** 例如：Switch(config-if)#**dot1x port-control auto**	在以上端口上启用 IEEE 802.1x 认证
8	**end** 例如：Switch(config-if)#**end**	返回特权模式

以下示例显示了如何在端口上启用周期性重认证功能，并且设置重认证周期为 4000 秒。

在 Cisco IOS 12.2(50)SG 及以后版本中的配置：

```
Switch#configure terminal
Switch(config)#interface fastethernet5/9
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#authentication periodic
Switch(config-if)#authentication timer reauthenticate 4000
Switch(config-if)#authentication port-control auto
Switch(config-if)#end
Switch#
```

在 Cisco IOS 12.2(46)SG 及以前版本中的配置：

```
Switch#configure terminal
Switch(config)#interface fastethernet5/9
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#dot1x reauthentication
Switch(config-if)#dot1x timeout reauth-period 4000
Switch(config-if)#dot1x port-control auto
Switch(config-if)#end
Switch#
```

23.2.12　启用多主机认证模式

可以为一个端口配置多主机认证模式，这样在端口被授权后，所有间接连接在该端口的主机（如通过连接另一个交换机再连接多个主机，或者 AP 连接多个 WLAN 主机）均获得访问网络的权限；如果该端口未被授权（重认证失败，或者没有收到 EAPOL-logoff 消息），交换机禁止所有间接连接在该端口上的主机访问网络。

多主机认证模式的配置步骤如表 23-14 所示。

表 23-14　多主机认证模式的配置步骤

步骤	命令	说明
1	**configure terminal** 例如：Switch#**configure terminal**	进入全局配置模式
2	**interface** *interface-id* 例如：Switch(config)#**interface** gigaethernet1/1	键入多个主机间接连接的交换机端口，进入接口配置模式
3	**switchport mode access** 例如：Switch(config-if)#**switchport mode access**	转换以上端口为二层访问模式端口
4	**dot1x pae authenticator** 例如：Switch(config-if)#**dot1x pae authenticator**	使用默认参数在以上端口上启用 IEEE 802.1x 认证
5	Cisco IOS 12.2(50)SG 及以后版本： **authentication host-mode multi-host** 例如：Switch(config-if)#**authentication host-mode multi-host** Cisco IOS 12.2(46)SG 及以前版本： **dot1x host-mode multi-host** 例如：Switch(config-if)#**dot1x host-mode multi-host**	指定以上端口为 IEEE 802.1x 多主机认证模式，可用 **no authentication host-mode multi-host** 接口配置模式命令（Cisco IOS 12.2(50)SG 及以后版本时）或者 **no dot1x host-mode multi-host** 接口配置模式命令（Cisco IOS 12.2(46)SG 及以前版本时）禁止多主机认证模式
6	Cisco IOS 12.2(50)SG 及以后版本： **authentication port-control auto** 例如：Switch(config-if)#**authentication port-control auto** Cisco IOS Release 12.2(46)SG 及以前版本： **dot1x port-control auto** 例如：Switch(config-if)#**dot1x port-control auto**	在以上端口上启用 IEEE 802.1x 认证
7	**end** 例如：Switch(config-if)#**end**	返回特权模式
8	**show dot1x interface** *interface-id* [**detail**] 例如：Switch#**show dot1x interface** gigaethernet1/1**detail**	校验以上配置
9	**copy running-config startup-config** 例如：Switch#**copy running-config startup-config**	（可选）保存以上配置到交换机启动配置文件中

以下示例显示的是如何在端口上启用 IEEE 802.1x 多主机认证模式。

在 Cisco IOS 12.2(50)SG 及以后版本中的配置：

```
Switch#configure terminal
Switch(config)#interface fastethernet5/9
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#authentication host-mode multi-host
Switch(config-if)#authentication port-control auto
Switch(config-if)#end
Switch#
```

在 Cisco IOS 12.2(46)SG 及以前版本中的配置：

```
Switch#configure terminal
Switch(config)#interface fastethernet5/9
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#dot1x host-mode multi-host
Switch(config-if)#dot1x port-control auto
Switch(config-if)#end
Switch#
```

23.2.13 修改静止周期

在交换机认证客户端失败，则交换机会在一个延时后重新对客户端进行认证。这个延时时间就是 quiet-period（静止周期）值。具体的配置步骤如表 23-15 所示。

表 23-15 静止周期修改配置步骤

步骤	命令	说明
1	**configure terminal** 例如：Switch#**configure terminal**	进入全局配置模式
2	**interface** *interface-id* 例如：Switch(config)#**interface** gigaethernet1/1	键入要配置静止周期的交换机端口，进入接口配置模式
3	**switchport mode access** 例如：Switch(config-if)#**switchport mode access**	转换以上端口为二层访问模式端口
4	**dot1x pae authenticator** 例如：Switch(config-if)#**dot1x pae authenticator**	使用默认参数在以上端口上启用 IEEE 802.1x 认证
5	**dot1x timeout quiet-period** *seconds* 例如：Switch(config-if)#**dot1x timeout quiet-period** 30	设置交换机在对客户端认证失败后再次重新认证所需等待的时间，取值范围为 0–65535 秒，默认值为 60 秒，可用 **no dot1x timeout quiet-period** 命令恢复为默认设置
6	Cisco IOS 12.2(50)SG 及以后版本： **authentication port-control auto** 例如：Switch(config-if)#**authentication port-control auto** Cisco IOS Release 12.2(46)SG 及以前版本： **dot1x port-control auto** 例如：Switch(config-if)#**dot1x port-control auto**	在以上端口上启用 IEEE 802.1x 认证
7	**end** 例如：Switch(config-if)#**end**	返回特权模式
8	**show dot1x all** 例如：Switch#**show dot1x all**	校验以上配置
9	**copy running-config startup-config** 例如：Switch#**copy running-config startup-config**	（可选）保存以上配置到交换机启动配置文件中

以下示例显示的是如何配置交换机 fastethernet4/1 端口重试客户端认证的等待时间为 30 秒。

在 Cisco IOS 12.2(50)SG 及以后版本中的配置：

```
Switch#configure terminal
Switch(config)#interface fastethernet4/1
```

```
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#dot1x timeout quiet-period 30
Switch(config-if)#authentication port-control auto
Switch(config-if)#end
Switch#
```

在 Cisco IOS 12.2(46)SG 及以前版本中的配置：

```
Switch#configure terminal
Switch(config)#interface fastethernet4/1
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#dot1x timeout quiet-period 30
Switch(config-if)#dot1x port-control auto
Switch(config-if)#end
Switch#
```

23.2.14　修改交换机到客户端的帧重传时间间隔和重传次数

客户端发送 EAP-Response/Identity 标识响应帧响应来自交换机的 EAP-Request/Identity 标识请求帧。如果交换机在等待一个时间间隔后仍收不到来自客户端的响应帧时，再次重发标识请求帧。这个等待的时间我们可以在交换机上配置，但建议不要修改默认值，仅需要对那些链路性能不好的客户端所连接端口的重传时间间隔进行改变。另外，还可以配置交换机在重新开始新的认证进程前，向客户端重传 EAP-Request/Identity 标识请求帧的最多次数。具体配置步骤如表 23-16 所示。

表 23-16　修改重传时间间隔和重传次数的配置步骤

步骤	命令	说明
1	**configure terminal** 例如：Switch#**configure terminal**	进入全局配置模式
2	**interface** *interface-id* 例如：Switch(config)#**interface** gigaethernet1/1	键入要配置静止周期的交换机端口，进入接口配置模式
3	**switchport mode access** 例如：Switch(config-if)#**switchport mode access**	转换以上端口为二层访问模式端口
4	**dot1x pae authenticator** 例如：Switch(config-if)#**dot1x pae authenticator**	使用默认参数在以上端口上启用 IEEE 802.1x 认证
5	**dot1x timeout tx-period** *seconds* 例如：Switch(config-if)#**dot1x timeout tx-period** 50	设置交换机在重传 EAP-Request/Identity 标识请求帧前，等待客户端响应的时间。取值范围为 1~65535 秒，默认值为 30 秒，可用 **no dot1x timeout tx-period** 命令恢复为默认设置
6	**dot1x max-req** *count* 例如：Switch(config-if)#**dot1x max-req** 3 或 **dot1x max-reauth-req** *count* 例如：Switch(config-if)#**dot1x max-reauth-req** 4	指定在没有收到来自客户端的 EAP-Response/Identity 标识响应帧时重传 EAP-Request/Identity 标识请求帧的最大次数，取值范围为 1~10 次，默认为 2 次。 可用 **no dot1x max-req** 或 **no dot1x max-reauth-req** 接口配置模式命令恢复为默认设置
7	Cisco IOS 12.2(50)SG 及以后版本： **authentication port-control auto** 例如：Switch(config-if)#**authentication port-control auto** Cisco IOS Release 12.2(46)SG 及以前版本： **dot1x port-control auto** 例如：Switch(config-if)#**dot1x port-control auto**	在以上端口上启用 IEEE 802.1x 认证
8	**end** 例如：Switch(config-if)#**end**	返回特权模式
9	**show dot1x all** 例如：Switch#**show dot1x all**	校验以上配置
10	**copy running-config startup-config** 例如：Switch#**copy running-config startup-config**	（可选）保存以上配置到交换机启动配置文件中

【示例 1】设置 fastethernet5/9 端口在没有接收到来自客户端的标识响应帧时，重传 EAP-Request/Identity 标识请求前所需等待的时间间隔为 60 秒。

在 Cisco IOS 12.2(50)SG 及以后版本中的配置：

```
Switch#configure terminal
Switch(config)#interface fastethernet5/9
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#dot1x timeout tx-period 60
Switch(config-if)#authentication port-control auto
Switch(config-if)#end
Switch#
```

在 Cisco IOS 12.2(46)SG 及以前版本中的配置：

```
Switch#configure terminal
Switch(config)#interface fastethernet5/9
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#dot1x timeout tx-period 60
Switch(config-if)#dot1x port-control auto
Switch(config-if)#end
Switch#
```

【示例 2】设置 fastethernet5/9 端口在没有接收到来自客户端的标识响应帧，开始新的认证进程前，重传 EAP-Request/Identity 标识请求帧的最多次数为 5。

在 Cisco IOS 12.2(50)SG 及以后版本中的配置：

```
Switch#configure terminal
Switch(config)#interface fastethernet5/9
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#dot1x max-reauth-req 5
Switch(config-if)#authentication port-control auto
Switch(config-if)#end
Switch#
```

在 Cisco IOS 12.2(46)SG 及以前版本中的配置：

```
Switch#configure terminal
Switch(config)#interface fastethernet5/9
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#dot1x max-reauth-req 5
Switch(config-if)#dot1x port-control auto
Switch(config-if)#end
Switch#
```