目 录

1 WLAN用户接入认证 ····· 1-1

1.1 WLAN用户接入认证配置命令 ····· 1-1

1.1.1 client url-redirect enable ····· 1-1

1.1.2 client-security accounting-delay time ····· 1-1

1.1.3 client-security accounting-restart trigger ipv4 ····· 1-2

1.1.4 client-security accounting-start trigger ····· 1-3

1.1.5 client-security accounting-update trigger ····· 1-4

1.1.6 client-security authentication critical-vlan ····· 1-5

1.1.7 client-security authentication fail-vlan ····· 1-6

1.1.8 client-security authentication-mode ····· 1-7

1.1.9 client-security authorization-fail offline ····· 1-8

1.1.10 client-security ignore-authentication ····· 1-9

1.1.11 client-security ignore-authorization ····· 1-10

1.1.12 client-security intrusion-protection action ····· 1-10

1.1.13 client-security intrusion-protection enable ····· 1-11

1.1.14 client-security intrusion-protection timer temporary-block ····· 1-12

1.1.15 client-security intrusion-protection timer temporary-service-stop ····· 1-13

1.1.16 display wlan client-security block-mac ····· 1-14

1.1.17 dot1x domain ····· 1-14

1.1.18 dot1x eap ····· 1-15

1.1.19 dot1x eap-termination eap-profile ····· 1-16

1.1.20 dot1x handshake enable ····· 1-17

1.1.21 dot1x handshake secure enable ····· 1-17

1.1.22 dot1x max-user ····· 1-18

1.1.23 dot1x re-authenticate enable ····· 1-19

1.1.24 mac-authentication domain ····· 1-20

1.1.25 mac-authentication max-user ····· 1-20

1.1.26 wlan authentication optimization ····· 1-21

1.1.27 wlan client-security authentication clear-previous-connection ····· 1-22

1 WLAN用户接入认证

1.1 WLAN用户接入认证配置命令

1.1.1 client url-redirect enable

client url-redirect enable 命令用来开启客户端 URL 重定向功能。

undo client url-redirect enable 命令用来关闭客户端 URL 重定向功能。

【命令】

client url-redirect enable

undo client url-redirect enable

【缺省情况】

客户端 URL 重定向功能处于关闭状态。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【使用指导】

该功能只能在无线服务模板处于关闭状态时配置。

本功能仅适用于客户端采用 RADIUS 服务器认证方式进行的 MAC 地址认证。

在用户进行 MAC 地址认证上线过程中，如果 RADIUS 服务器上没有记录用户及其 MAC 地址的对应信息，但仍需要用户进行认证时，可以通过在设备上开启 URL 重定向功能。开启后，用户可以根据 RADIUS 服务器下发的重定向 URL，跳转到指定的 Web 认证界面进行用户认证。用户认证通过后，RADIUS 服务器将记录用户的 MAC 地址信息，并通过 DM 报文强制用户下线，此后该用户即可正常完成 MAC 地址认证。有关 DM 报文的详细介绍请参见“用户接入与认证配置指导”中的“AAA”。

【举例】

在无线服务模板 service1 下开启客户端 URL 重定向功能。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] client url-redirect enable
```

1.1.2 client-security accounting-delay time

client-security accounting-delay time 命令用来开启计费延时功能。

undo client-security accounting-delay time 命令用来恢复缺省情况。

【命令】

client-security accounting-delay time *time* [**no-ip-logoff**]

undo client-security accounting-delay time

【缺省情况】

学习到无线客户端的 IP 地址后，才会向计费服务器发起计费开始请求。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

time *time*：计费延时的时长，取值范围为 1～600，单位为秒。

no-ip-logoff：如果设备在指定的延时时间内没有获取到无线客户端 IP 地址，则让客户端下线。若不指定该参数，则设备在指定计费延时时间到达后，将会发送计费开始请求报文。

【使用指导】

如果在指定的计费延时时间内设备没有学习到指定类型客户端的 IP 地址，则执行相应的计费延时动作。触发计费开始的无线客户端 IP 地址类型由 **client-security accounting-start trigger** 命令的配置决定，当客户端 IP 地址类型为 none 时，计费延时功能不生效。

建议根据设备获取 IP 地址的时长来配置计费延时的时长，若网络环境较差，设备需要较长的时间获取到 IP 地址，则可适当增大该值。

无线服务模板开启后，再配置本特性，则配置只对新上线的客户端生效，对已经上线的客户端无效。

【举例】

在无线服务模板 service1 下，配置计费延时时间为 15 秒。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] client-security accounting-delay time 15 no-ip-logoff
```

【相关命令】

- **client-security accounting-start trigger**

1.1.3 client-security accounting-restart trigger ipv4

client-security accounting-restart trigger ipv4 命令用来开启 IPv4 地址变化客户端的重新计费功能。

undo client-security accounting-restart trigger ipv4 命令用来恢复缺省情况。

【命令】

client-security accounting-restart trigger ipv4

undo client-security accounting-restart trigger ipv4

【缺省情况】

IPv4 地址变化客户端的重新计费功能处于关闭状态。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【使用指导】

通过 **client-security accounting-update trigger** 命令配置触发计费更新的无线客户端 IP 地址类型为 IPv4 后，当客户端 IPv4 地址发生变化时，设备就会立即向计费服务器发送计费更新报文，对客户端进行重新计费；开启本功能后，当客户端 IPv4 地址发生变化时，首先设备会立即向计费服务器发送计费停止报文，然后再重新向计费服务器发送计费开始报文，对客户端进行重新计费。

client-security accounting-restart trigger ipv4 命令的优先级高于 **client-security accounting-update trigger** 命令。

本命令只能在无线服务模板处于关闭状态时配置。

【举例】

在无线服务模板 service1 下，开启 IPv4 地址变化客户端的重新计费功能。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] client-security accounting-restart trigger ipv4
```

1.1.4 client-security accounting-start trigger

client-security accounting-start trigger 命令用来配置触发计费开始的无线客户端 IP 地址类型。

undo client-security accounting-start trigger 命令用来恢复缺省情况。

【命令】

client-security accounting-start trigger { **ipv4** | **ipv4-ipv6** | **ipv6** | **none** }

undo client-security accounting-start trigger

【缺省情况】

触发计费开始的无线客户端 IP 地址类型为 IPv4。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

ipv4：表示无线客户端 IP 地址类型为 IPv4。

ipv4-ipv6：表示无线客户端 IP 地址类型为 IPv4 或 IPv6。

ipv6：表示无线客户端 IP 地址类型为 IPv6。

none：表示设备在无线客户端认证成功后就会发送计费开始请求报文。

【使用指导】

无线客户端通过 802.1X 认证或者 MAC 地址认证方式上线后，设备会根据触发计费开始的无线客户端 IP 地址类型决定是否向计费服务器发送计费开始请求报文，当计费服务器返回计费开始响应报文后开始对客户端进行计费。

配置触发计费开始的无线客户端 IP 地址类型时，需要开启相应类型的客户端地址学习功能，配置才会生效，否则无法触发计费开始。有关客户端地址学习功能的详细介绍请参见“用户接入与认证配置指导”中的“WLAN IP Snooping”。

本命令配置的无线客户端 IP 地址类型需要满足计费服务器的协议要求。

无线服务模板开启后，再配置本特性，新配置只对新上线的客户端生效，对已经上线的客户端无效。

【举例】

在无线服务模板 service1 下，配置触发计费开始的无线客户端 IP 地址类型为 IPv4。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] client-security accounting-start trigger ipv4
```

【相关命令】

- **client ipv4-snooping arp-learning enable**（用户接入与认证命令参考/WLAN IP Snooping）
- **client ipv4-snooping dhcp-learning enable**（用户接入与认证命令参考/WLAN IP Snooping）
- **client ipv6-snooping dhcpv6-learning enable**（用户接入与认证命令参考/WLAN IP Snooping）
- **client ipv6-snooping nd-learning enable**（用户接入与认证命令参考/WLAN IP Snooping）
- **client ipv6-snooping snmp-nd-report enable**（用户接入与认证命令参考/WLAN IP Snooping）
- **client-security accounting-delay**
- **client-security accounting-update trigger**

1.1.5 client-security accounting-update trigger

client-security accounting-update trigger 命令用来配置触发计费更新的无线客户端 IP 地址类型。

undo client-security accounting-update trigger 命令用来恢复缺省情况。

【命令】

client-security accounting-update trigger { **ipv4** | **ipv4-ipv6** | **ipv6** }

undo client-security accounting-update trigger

【缺省情况】

根据计费服务器下发或设备配置的实时计费的时间间隔周期性发送计费更新请求报文。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

ipv4：表示无线客户端 IP 地址类型为 IPv4，设备仅在学习到客户端 IPv4 地址变化时才会发送计费更新请求报文。

ipv4-ipv6：表示无线客户端 IP 地址类型为 IPv4 或 IPv6，设备只要学习到客户端 IP 地址变化就会发送计费更新请求报文。

ipv6：表示无线客户端 IP 地址类型为 IPv6，设备仅在学习到客户端 IPv6 地址变化时才会发送计费更新请求报文。

【使用指导】

仅当触发计费开始的无线客户端 IP 地址类型配置生效时，触发计费更新的无线客户端 IP 地址类型的配置才会生效。

当完成该配置后，该配置和周期性发送计费更新报文功能同时生效。

假设配置的触发计费更新的无线客户端 IP 地址类型为 IPv6，周期性发送计费更新报文功能配置的实时计费间隔为 12 分钟（**timer realtime-accounting** 命令配置），则设备会每隔 12 分钟发起一次计费更新请求，且当在线客户端 IPv6 地址发生变化时，设备也会立即发送计费更新请求报文。

无线服务模板开启后，再配置本特性，则配置只对新上线的客户端生效，对已经上线的客户端无效。

【举例】

在无线服务模板下，配置触发计费更新的客户端 IP 地址类型为 IPv4。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] client-security accounting-update trigger ipv4
```

【相关命令】

- **client-security accounting-start trigger**
- **timer realtime-accounting**（用户接入与认证命令参考/AAA）

1.1.6 client-security authentication critical-vlan

client-security authentication critical-vlan 命令用来配置服务模板下的 Critical VLAN。

undo client-security authentication critical-vlan 命令用来恢复缺省情况。

【命令】

client-security authentication critical-vlan *vlan-id*

undo client-security authentication critical-vlan

【缺省情况】

未配置 Critical VLAN。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

vlan-id：Critical VLAN 的 VLAN ID，取值范围为 1～4094。

【使用指导】

Critical VLAN 功能允许用户在认证时，当所有认证服务器都不可达的情况下访问某一特定 VLAN 中的资源，这个 VLAN 称之为 Critical VLAN。配置 Critical VLAN 后，当用户认证时，若所有认证服务器都不可达，则用户将被加入该 VLAN，同时设备会启动一个 30 秒的定时器，以定期对用户进行重新认证：

- 如果重认证通过，设备会根据授权服务器是否下发 VLAN 来重新指定该用户所在 VLAN。即如果授权服务器下发了 VLAN，则该用户将被加入该下发的 VLAN，否则该用户将被加入其原来所属的 VLAN。
- 如果重认证未通过，当认证服务不可达时，用户仍然仅可访问 Critical VLAN 中的资源，当认证服务器可达但因某种原因明确拒绝用户认证通过，且配置了 Fail VLAN 时，用户可以访问 Fail VLAN 中的资源。

需要注意的是，如果采用 RSNA 安全机制的 802.1X 用户认证时所有认证服务器都不可达，则用户会直接下线，不会加入 Critical VLAN。

本命令只能在无线服务模板处于关闭状态时配置。

【举例】

在无线服务模板 service1 下配置 Critical VLAN 为 VLAN 10。

```
<Sysname> sysname-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] client-security authentication critical-vlan 10
```

1.1.7 client-security authentication fail-vlan

client-security authentication fail-vlan 命令用来配置服务模板下的认证失败 VLAN。

undo client-security authentication fail-vlan 命令用来恢复缺省情况。

【命令】

client-security authentication fail-vlan *vlan-id*

undo client-security authentication fail-vlan

【缺省情况】

未配置认证失败 VLAN。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

vlan-id：认证失败 VLAN 的 VLAN ID，取值范围为 1～4094。

【使用指导】

这里的认证失败是认证服务器因某种原因明确拒绝用户认证通过，比如用户密码错误，而不是认证超时或网络连接等原因造成的认证失败。

配置认证失败的 VLAN 必须是已经存在的 VLAN。

本命令只能在无线服务模板处于关闭状态时配置。

【举例】

在无线服务模板 1 下配置认证失败 VLAN 为 VLAN 10。

```
<Sysname> sysname-view
[Sysname] wlan service-template 1
[Sysname-wlan-st-1] client-security authentication fail-vlan 10
```

1.1.8 client-security authentication-mode

client-security authentication-mode 命令用来配置无线用户接入认证模式。

undo client-security authentication-mode 命令用来恢复缺省情况。

【命令】

client-security authentication-mode { **dot1x** | **dot1x-then-mac** | **mac** | **mac-then-dot1x** | **oui-then-dot1x** }

undo client-security authentication-mode

【缺省情况】

不对用户进行接入认证即 Bypass 认证。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

dot1x：表示只进行 802.1X 认证。

dot1x-then-mac：表示先进行 802.1X 认证，如果失败，再进行 MAC 地址认证。如果认证成功，则不进行 MAC 地址认证。

mac：表示只进行 MAC 地址认证。

mac-then-dot1x：表示先进行 MAC 地址认证，如果失败，再进行 802.1X 认证。如果认证成功，则不进行 802.1X 认证。

oui-then-dot1x：表示先进行 OUI 认证，如果失败，再进行 802.1X 认证。如果认证成功，则不进行 802.1X 认证。

【使用指导】

以上各模式下，每个无线服务模板上均允许接入多个认证通过的用户。802.1X 用户的数目由 **dot1x max-user** 命令配置，MAC 地址认证用户的数目由 **mac-authentication max-user** 命令配置。

本命令只能在无线服务模板处于关闭状态时配置。

【举例】

在无线服务模板 service1 下配置无线用户接入认证模式为 MAC 地址认证模式。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] client-security authentication-mode mac
```

1.1.9 client-security authorization-fail offline

client-security authorization-fail offline 命令用来开启授权失败后的用户下线功能。

undo client-security authorization-fail offline 命令用来关闭授权失败后的用户下线功能。

【命令】

client-security authorization-fail offline

undo client-security authorization-fail offline

【缺省情况】

授权失败后的用户下线功能处于关闭状态。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【使用指导】

如果开启了授权失败后的用户下线功能，当下发的授权 ACL、User Profile 不存在、已授权 ACL、User Profile 被删除，或者 ACL、User Profile 下发失败时，将强制用户下线；

如果没有开启授权失败后的用户下线功能，当下发的授权 ACL、User Profile 不存在、已授权 ACL、User Profile 被删除，或者 ACL、User Profile 下发失败时，用户保持在线，授权 ACL、User Profile 不生效，设备打印 Log 信息。

本命令只能在无线服务模板处于关闭状态时配置。

【举例】

在无线服务模板 service1 下开启授权失败用户下线功能。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] client-security authorization-fail offline
```

1.1.10 client-security ignore-authentication

client-security ignore-authentication 命令用来配置忽略 802.1X 或 MAC 地址认证结果。

undo client-security ignore-authentication 命令用来恢复缺省情况。

【命令】

client-security ignore-authentication

undo client-security ignore-authentication

【缺省情况】

对于 802.1X 认证方式的无线用户，应用 802.1X 认证结果；对于通过 RADIUS 服务器进行远程 MAC 地址认证的无线用户，应用 MAC 地址认证结果。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【使用指导】

本功能仅适用于采用 802.1X 认证方式的无线用户以及通过 RADIUS 服务器进行远程 MAC 地址认证+Portal 认证的无线用户。

若某无线服务模板下有漫游的 RSN+802.1X 认证方式的无线用户上线，请勿配置本功能，否则会导致漫游失败。

本功能适用于以下两种用户：

- 对于 802.1X 认证的无线用户，开启本功能后，当 802.1X 认证失败时，设备会忽略这一认证结果，允许用户访问网络资源。
- 对于通过 RADIUS 服务器进行远程 MAC 地址认证+Portal 认证的无线用户，需要依次通过 MAC 地址认证和 Portal 认证才能访问网络资源，且每次都需要输入 Portal 用户名和密码。配置本功能后，可以简化上述认证过程。简化后的认证过程如下：
  - 若 RADIUS 服务器上已经记录了用户和客户端 MAC 地址的对应信息，判断用户通过 MAC 地址认证，且不需要进行 Portal 认证即可访问网络资源。
  - 若 RADIUS 服务器上未记录用户和客户端 MAC 地址的对应信息，判断 MAC 地址认证失败。此时，设备忽略这一认证结果，直接进行 Portal 认证。Portal 认证通过后即可访问网络资源，同时 RADIUS 服务器将记录该用户和客户端 MAC 地址的对应信息。

本功能只能在无线服务模板处于关闭的状态下进行配置。

【举例】

在无线服务模板 service1 下配置忽略 802.1X 或 MAC 地址认证的结果。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] client-security ignore-authentication
```

1.1.11 client-security ignore-authorization

client-security ignore-authorization 命令用来配置忽略 RADIUS 服务器或设备本地下发的授权信息。

undo client-security ignore-authorization 命令用来恢复缺省情况。

【命令】

client-security ignore-authorization

undo client-security ignore-authorization

【缺省情况】

应用 RADIUS 服务器或设备本地下发的授权信息。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【使用指导】

当用户通过 RADIUS 认证或本地认证后，RADIUS 服务器或设备会根据用户帐号配置的相关属性进行授权，比如动态下发 VLAN 等。若不希望接受这类动态下发的授权属性，则可通过配置本命令来忽略。

本命令只能在无线服务模板处于关闭状态时配置。

【举例】

在无线服务模板 service1 下配置忽略 RADIUS 服务器或设备本地下发的授权信息。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] client-security ignore-authorization
```

1.1.12 client-security intrusion-protection action

client-security intrusion-protection action 命令用来配置当接收到非法报文时采取的入侵检测模式。

undo client-security intrusion-protection action 命令用来恢复缺省情况。

【命令】

client-security intrusion-protection action { service-stop | temporary-block | temporary-service-stop }

undo client-security intrusion-protection action

【缺省情况】

入侵检测模式为 **temporary-block** 模式。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

service-stop：直接关闭收到非法报文的 BSS 提供的所有服务。用户可以手工在 Radio 口上重新生成该 BSS 使得用户正常接入。

temporary-block：临时将用户 MAC 加入阻塞 MAC 列表中。临时阻止非法用户上线的时间由 **client-security intrusion-protection timer temporary-block** 命令配置。

temporary-service-stop：临时将收到非法报文的 BSS 所提供的所有服务关闭。临时关闭收到非法报文的 BSS 所提供服务的时间由 **client-security intrusion-protection timer temporary-service-stop** 命令配置。

【使用指导】

本命令只能在无线服务模板处于关闭状态时配置。

只有开启入侵检测功能后，入侵检测措施才生效。开启入侵检测功能由 **client-security intrusion-protection enable** 命令配置。

【举例】

在无线服务模板 service1 下配置入侵检测措施为 **service-stop**。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] client-security intrusion-protection enable
[Sysname-wlan-st-service1] client-security intrusion-protection action service-stop
```

【相关命令】

- **client-security intrusion-protection enable**
- **client-security intrusion-protection timer temporary-block**
- **client-security intrusion-protection timer temporary-service-stop**

1.1.13 client-security intrusion-protection enable

client-security intrusion-protection enable 命令用来开启入侵检测功能。

undo client-security intrusion-protection enable 命令用来关闭入侵检测功能。

【命令】

client-security intrusion-protection enable

undo client-security intrusion-protection enable

【缺省情况】

入侵检测功能处于关闭状态。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【使用指导】

当设备检测到一个认证失败的用户试图通过该无线服务模板绑定的 BSS（基本服务集）接入时，如果入侵检测功能处于开启状态，则设备将对其所在的 BSS 采取相应的安全措施。具体的安全措施由 **client-security intrusion-protection action** 命令指定。

本命令只能在无线服务模板处于关闭状态时配置。

【举例】

在无线服务模板 service1 下开启入侵检测功能。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] client-security intrusion-protection enable
```

【相关命令】

- **client-security intrusion-protection action**

1.1.14 client-security intrusion-protection timer temporary-block

client-security intrusion-protection timer temporary-block 命令用来配置临时阻塞非法入侵用户的时长。

undo client-security intrusion-protection timer temporary-block 命令用来恢复缺省情况。

【命令】

client-security intrusion-protection timer temporary-block *time*

undo client-security intrusion-protection timer temporary-block

【缺省情况】

临时阻塞非法入侵用户时间为 180 秒。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

time：临时阻塞非法入侵用户时长，取值范围为 60～300，单位为秒。

【使用指导】

当入侵检测功能处于使能状态且入侵检测措施为临时阻塞非法用户（**temporary-block**）时，如果用户认证失败，则在该配置所指定的时间范围内，源 MAC 地址为此非法 MAC 地址的用户将无法认证成功，在这段时间之后恢复正常。

当无线服务模板使能后，若修改临时阻塞非法用户的时长，则新的配置在原有定时器超时后生效。

【举例】

在无线服务模板 service1 下配置临时阻塞非法入侵用户时长为 120 秒。

```
<Sysname> system-view
[Sysname] wlan service-template service1
```

```
[Sysname-wlan-st-service1] client-security intrusion-protection enable
[Sysname-wlan-st-service1] client-security intrusion-protection action temporary-block
[Sysname-wlan-st-service1] client-security intrusion-protection timer temporary-block 120
```

【相关命令】

- **client-security intrusion-protection enable**
- **client-security intrusion-protection action**

1.1.15 client-security intrusion-protection timer temporary-service-stop

client-security intrusion-protection timer temporary-service-stop 命令用来配置临时关闭 BSS 服务的时长。

undo client-security intrusion-protection timer temporary-service-stop 命令用来恢复缺省情况。

【命令】

client-security intrusion-protection timer temporary-service-stop *time*

undo client-security intrusion-protection timer temporary-service-stop

【缺省情况】

临时关闭 BSS 服务时长为 20 秒。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

time：临时关闭 BSS 服务的时长，取值范围为 10～300，单位为秒。

【使用指导】

当入侵检测功能处于使能状态，且入侵检测措施为临时关闭服务（**temporary-service-stop**）时，如果设备检测到非法报文，则在该配置指定的时间段内关闭用户所在的 BSS 所提供的所有服务，在此期间用户将无法通过该服务接入网络，这段时间之后恢复正常。

当无线服务模板使能后，若修改临时关闭 BSS 服务的时长，则新的配置在原有定时器超时后生效。

【举例】

在无线服务模板 service1 下配置临时关闭 BSS 服务的时长为 30 秒。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] client-security intrusion-protection enable
[Sysname-wlan-st-service1] client-security intrusion-protection action
temporary-service-stop
[Sysname-wlan-st-service1] client-security intrusion-protection timer
temporary-service-stop 30
```

【相关命令】

- **client-security intrusion-protection enable**

- **client-security intrusion-protection action**

1.1.16 display wlan client-security block-mac

display wlan client-security block-mac 命令用来显示阻塞 MAC 地址信息。

【命令】

display wlan client-security block-mac

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【使用指导】

阻塞 MAC 是指入侵检测模式为 **temporary-block** 时，被加入到阻塞 MAC 列表中的用户。

【举例】

显示所有阻塞 MAC 地址信息。

```
<Sysname> display wlan client-security block-mac
MAC address         AP ID       RADIO ID     BSSID
0002-0002-0002      1           1            00ab-0de1-0001
000d-88f8-0577      1           1            0ef1-0001-02c1

Total entries: 2
```

表1-1 display wlan client-security block-mac 命令显示信息描述表

字段	描述
MAC address	阻塞MAC地址，格式为“H-H-H”
AP ID	阻塞MAC地址所在AP的编号
RADIO ID	阻塞MAC地址所在的Radio编号
BSSID	基本服务集标识符，格式为H-H-H
Total entries	阻塞MAC地址表项条数

【相关命令】

- **client-security instrusion-protection action**
- **client-security instrusion-protection timer temporary-block**

1.1.17 dot1x domain

dot1x domain 命令用来指定无线服务模板下 802.1X 用户的认证域。

undo dot1x domain 命令用来恢复缺省情况。

【命令】

dot1x domain *domain-name*

undo dot1x domain

【缺省情况】

未指定无线服务模板下的 802.1X 用户的 ISP 域。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

domain-name：ISP 域名，为 1～255 个字符的字符串，不区分大小写。

【使用指导】

本命令只能在无线服务模板处于关闭状态时配置。

从无线服务模板上接入的 802.1X 用户将按照如下先后顺序进行选择认证域：无线服务模板下指定的认证域-->用户名中指定的认证域-->系统缺省的认证域。

【举例】

配置无线服务模板 service1 下 802.1X 用户使用认证域为 my-domain。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] dot1x domain my-domain
```

1.1.18 dot1x eap

dot1x eap 命令用来配置 802.1X 认证的 EAP 协议模式。

undo dot1x eap 命令用来恢复缺省情况。

【命令】

dot1x eap { **extended** | **standard** }

undo dot1x eap

【缺省情况】

EAP 协议模式为 **standard**。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

extended：表示 EAP 协议模式为扩展的 EAP 协议，即要求客户端和设备按照私有 EAP 协议的规范和报文格式进行交互。

standard：表示 EAP 协议模式为标准的 EAP 协议，即要求客户端和设备按照标准 EAP 协议的规范和报文格式进行交互。

【使用指导】

只能在无线服务模板关闭的状态下开启该功能。

【举例】

在无线服务模板 1 下配置 802.1X 认证的 EAP 协议为扩展模式。

```
<Sysname> system-view
[Sysname] wlan service-template 1
[Sysname-wlan-st-1] dot1x eap extended
```

1.1.19 dot1x eap-termination eap-profile

dot1x eap-termination eap-profile 命令用来配置 802.1X 认证采用 EAP 终结方式时引用的 EAP 认证方案。

undo dot1x eap-termination eap-profile 命令用来恢复缺省情况。

【命令】

dot1x eap-termination eap-profile *eap-profile-name*

undo dot1x eap-termination eap-profile

【缺省情况】

未配置 802.1X 认证采用 EAP 终结方式时引用的 EAP 认证方案。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

eap-profile-name：EAP 认证方案名称，为 1～32 个字符的字符串，不区分大小写。引用的 EAP 认证方案名称必须已经存在。

【使用指导】

当客户端使用了 RADIUS 服务器不支持的认证方法，并采用 EAP 中继方式进行认证，造成认证失败时，可以配置本命令，设备采用 EAP 终结方式将客户端认证请求报文封装在标准 RADIUS 报文中发送给认证服务器，从而使客户端通过认证。

目前本命令仅支持采用 PEAP-GTC 认证方式的认证请求报文进行处理。

【举例】

配置 802.1X 认证采用 EAP 终结方式时引用的 EAP 认证方案为 gtcprofile。

```
<Sysname> system-view
[Sysname] wlan service-template srvtmp1
[Sysname-wlan-st-srvtmp1] dot1x eap-termination eap-profile gtcprofile
```

【相关命令】

- **eap-profile**（安全命令参考/AAA）

- method（安全命令参考/AAA）
- **ssl-server-policy**

1.1.20 dot1x handshake enable

dot1x handshake enable 命令用来开启 802.1X 在线用户握手功能。

undo dot1x handshake enable 命令用来关闭 802.1X 在线用户握手功能。

【命令】

dot1x handshake enable

undo dot1x handshake enable

【缺省情况】

802.1X 在线用户握手功能处于关闭状态。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【使用指导】

使能 802.1X 握手功能之后，设备将定期向通过 802.1X 认证的在线用户发送握手报文，即单播 EAP-Request/Identity 报文，来检测用户的在线状态。握手报文发送的时间间隔由 802.1X 握手定时器控制（时间间隔通过命令 **dot1x timer handshake-period** 设置）。如果连续发送握手报文的次数达到 802.1X 报文最大重发次数（最大重发次数通过命令 **dot1x retry** 设置），而还没有收到用户响应，则强制该用户下线。

本命令只能在无线服务模板处于关闭状态时配置。

【举例】

开启无线服务模板 service1 下的 802.1X 在线用户握手功能。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] dot1x handshake enable
```

【相关命令】

- **dot1x handshake secure enable**
- **dot1x retry**（用户接入与认证命令参考-802.1X）
- **dot1x timer handshake-period**（用户接入与认证命令参考-802.1X）

1.1.21 dot1x handshake secure enable

dot1x handshake secure enable 命令用来开启 802.1X 在线用户安全握手功能。

undo dot1x handshake secure enable 命令用来关闭 802.1X 在线用户安全握手功能。

【命令】

dot1x handshake secure enable

undo dot1x handshake secure enable

【缺省情况】

802.1X 在线用户的安全握手功能处于关闭状态。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【使用指导】

本命令只能在无线服务模板处于关闭状态时配置。

802.1X 安全握手功能只有在开启了 802.1X 握手功能的前提下才生效。

该命令只对进行 802.1X 接入认证且成功上线的用户有效。

【举例】

开启无线服务模板 service1 下的 802.1X 在线用户安全握手功能。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] dot1x handshake enable
[Sysname-wlan-st-service1] dot1x handshake secure enable
```

【相关命令】

- **dot1x handshake enable**

1.1.22 dot1x max-user

dot1x max-user 命令用来配置无线服务模板上的 802.1X 最大用户数。

undo dot1x max-user 命令用来恢复缺省情况。

【命令】

dot1x max-user *count*

undo dot1x max-user

【缺省情况】

无线服务模板上允许同时接入的 802.1X 用户数为 4096 个。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

count：无线服务模板上最多允许同时接入的 802.1X 用户数，取值范围为 1～4096。

【使用指导】

本命令只能在无线服务模板处于关闭状态时配置。

配置本命令后，当接入此无线服务模板的 802.1X 用户数超过最大值后，新的用户将被拒绝。

【举例】

配置无线服务模板 service1 上的 802.1X 最大用户数为 500。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] dot1x max-user 500
```

1.1.23 dot1x re-authenticate enable

dot1x re-authenticate enable 命令用来开启 802.1X 周期性重认证功能。

undo dot1x re-authenticate enable 命令用来关闭 802.1X 周期性重认证功能。

【命令】

dot1x re-authenticate enable

undo dot1x re-authenticate enable

【缺省情况】

802.1X 周期性重认证功能处于关闭状态。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【使用指导】

无线服务模板启动了 802.1X 的周期性重认证功能后，设备会根据系统视图下配置的周期性重认证定时器（**dot1x timer reauth-period**）时间间隔对在线 802.1X 用户启动认证，以检测用户连接状态的变化，更新服务器下发的授权属性（例如 ACL，VLAN，User Profile）。

用户进行 802.1X 认证成功后，如果服务器下发了 Termination action 和 Session timeout 属性（**display dot1x connection**），且 Termination action 取值为 Radius-Request，Session timeout 取值不为 0，设备将以 Session timeout 为周期对用户进行重认证，以检测用户在线状态，并更新授权信息。

本命令只能在无线服务模板处于关闭状态时配置。

在认证服务器没有下发 Terminal action 和 Session timeout 属性或下发的 Terminal action 取值不为 Request 的情况下，如果使能 802.1X 重认证功能，设备也会定期向已经在线的 802.1X 用户发起重认证，此时重认证周期由 802.1X 重认证定时器配置。

【举例】

开启无线服务模板 service1 下的 802.1X 重认证功能。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] dot1x re-authenticate enable
```

【相关命令】

- **dot1x timer**（用户接入与认证命令参考-802.1X）

1.1.24 mac-authentication domain

mac-authentication domain 命令用来指定无线服务模板下 MAC 地址认证用户的 ISP 域。

undo mac-authentication domain 命令用来恢复缺省情况。

【命令】

mac-authentication domain *domain-name*

undo mac-authentication domain

【缺省情况】

未指定无线服务模板下的 MAC 地址认证用户的 ISP 域。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

domain-name：ISP 域名，为 1～255 个字符的字符串，不区分大小写。

【使用指导】

本命令只能在无线服务模板处于关闭状态时配置。

从无线服务模板上接入的 MAC 地址认证用户将按照如下先后顺序进行选择 ISP 域：无线服务模板下指定的 ISP 域-->全局 MAC 地址 ISP 域-->系统缺省的 ISP 域。

【举例】

配置无线服务模板 service1 下 MAC 地址认证用户使用的 ISP 域为 my-domain。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] mac-authentication domain my-domain
```

1.1.25 mac-authentication max-user

mac-authentication max-user 命令用来配置无线服务模板上的 MAC 地址认证最大用户数。

undo mac-authentication max-user 命令用来恢复缺省情况。

【命令】

mac-authentication max-user *count*

undo mac-authentication max-user

【缺省情况】

无线服务模板上允许接入的 MAC 地址认证最大用户数为 4096 个。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

count：可接入无线服务模板的 MAC 地址认证用户个数，取值范围为 1～4096。

【使用指导】

本命令只能在无线服务模板处于关闭状态时配置。

配置本命令后，当接入此无线服务模板的 MAC 地址认证用户数超过最大值后，新接入的用户将被拒绝。

【举例】

配置最大接入 MAC 地址认证用户数为 32 个。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] mac-authentication max-user 32
```

1.1.26 wlan authentication optimization

wlan authentication optimization 命令用来配置 802.1X 认证、MAC 地址认证及二层 Portal 认证的认证成功率、在线用户异常下线率的优化参数值。

undo wlan authentication optimization 命令用来恢复缺省情况。

【命令】

wlan authentication optimization *value*

undo wlan authentication optimization

【缺省情况】

802.1X 认证、MAC 地址认证及二层 Portal 认证的认证成功率、在线用户异常下线率的优化参数值为 0，即不对 802.1X 认证、MAC 地址认证及二层 Portal 认证的认证成功率、在线用户异常下线率进行优化，采用实际值。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

value：优化 802.1X 认证、MAC 地址认证及二层 Portal 认证的认证成功率、在线用户异常下线率的参数值，取值范围为 900～1000。该数值配置越小，802.1X 认证、MAC 地址认证及二层 Portal 认证的认证成功率越小，在线用户异常下线率越大。

【使用指导】

认证成功率是指 802.1X 认证、MAC 地址认证及二层 Portal 认证时认证成功的总次数占认证总次数的百分比。在线用户异常下线率是指在线用户异常断开连接的总次数占在线用户认证成功的总次数与当前在线用户总数之和的百分比。

设备会重新对 802.1X 认证、MAC 地址认证及二层 Portal 认证的认证成功率、在线用户异常下线率进行优化计算。

只有 802.1X 认证、MAC 地址认证及二层 Portal 认证采用 RADIUS 服务器进行远程认证时，本命令配置的优化参数才会生效。

【举例】

配置 802.1X 认证、MAC 地址认证及二层 Portal 认证的认证成功率、在线用户异常下线率的优化参数值为 950。

```
<Sysname> system-view
[Sysname] wlan authentication optimization 950
```

1.1.27 wlan client-security authentication clear-previous-connection

wlan client-security authentication clear-previous-connection 命令用来开启已认证无线客户端再次上线认证清除旧连接功能。

undo wlan client-security authentication clear-previous-connection 命令用来关闭已认证无线客户端再次上线认证清除旧连接功能。

【命令】

wlan client-security authentication clear-previous-connection

undo wlan client-security authentication clear-previous-connection

【缺省情况】

已认证无线客户端再次上线认证清除旧连接功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

当无线客户端进行 802.1X 或者 MAC 地址认证时，设备会检查自身是否存在该无线客户端的表项：

- 当不存在该无线客户端表项时，客户端进行认证上线。
- 当存在该无线客户端表项时，设备会删除该无线客户端的表项并向 RADIUS 服务器发送认证请求报文。有一些 RADIUS 服务器收到认证请求报文后，若发现本地已经存在该无线客户端的表项，会向设备回复认证失败的报文，导致客户端无法通过认证上线。

为了解决此类 RADIUS 服务器上因表项冲突而导致用户无法上线的问题，建议开启本功能。开启本功能后，设备存在表项的同时会向 RADIUS 服务器发送计费停止报文。当 RADIUS 服务器收到该报文后，会删除本地存在的无线客户端表项，客户端可以进行认证上线。

需要注意的是，开启本功能后，802.1X 重认证功能、Fail VLAN 功能和 Critical VLAN 功能将不能生效。

【举例】

开启已认证无线客户端再次上线认证清除旧连接功能。

```
<Sysname> system-view
[Sysname] wlan client-security authentication clear-previous-connection
```