目 录

1 WLAN用户安全

1.1 WLAN用户安全配置命令

1.1.1 akm mode

akm mode 命令用来配置身份认证与密钥管理的模式。

undo akm mode 命令用来恢复缺省情况。

【命令】

akm mode { **dot1x** | **private-psk** | **psk** }

undo akm mode

【缺省情况】

未配置身份认证与密钥管理。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

dot1x：表示身份认证与密钥管理的模式是 802.1X 模式。

private-psk：表示身份认证与密钥管理的模式是 Private-PSK 模式。

psk：表示身份认证与密钥管理的模式是 PSK 模式。

【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，并且只能配置一种模式。

当 WLAN 网络采用 RSNA 安全机制时，必须配置身份认证与密钥管理。

每一种身份认证模式都有互相依赖的用户认证方式：

- 802.1X 模式和 802.1X 用户认证模式相互依赖，必须同时配置。有关 802.1X 的详细介绍请参见“用户接入与认证配置指导”中的“WLAN 用户接入认证”。
- Private-PSK 模式和 MAC 地址认证模式相互依赖，必须同时配置，有关 MAC 地址认证的详细介绍请参见“用户接入与认证配置指导”中的“WLAN 用户接入认证”。
- PSK 模式和 MAC 地址认证模式或 Bypass 用户认证模式相互依赖，必须同时配置。有关 MAC 地址认证和 Bypass 认证的详细介绍请参见“用户接入与认证配置指导”中的“WLAN 用户接入认证”。

【举例】

配置身份认证与密钥管理模式为 PSK 模式。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] akm mode psk
```

【相关命令】

- **cipher-suite**
- **security-ie**

1.1.2 cipher-suite

cipher-suite 命令用来配置在帧加密时使用的加密套件。

undo cipher-suite 命令用来取消在帧加密时使用指定的加密套件。

【命令】

cipher-suite { ccmp | tkip | wep40 | wep104 | wep128 }

undo cipher-suite { ccmp | tkip | wep40 | wep104 | wep128 }

【缺省情况】

未配置加密套件。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

ccmp：AES-CCMP 加密套件。

tkip：TKIP 加密套件。

wep40：WEP40 加密套件。

wep104：WEP104 加密套件。

wep128：WEP128 加密套件。

【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。

如果配置了安全 IE，则必须配置 TKIP 或者 CCMP 加密套件中的一种。当 WLAN 网络采用 RSNA 安全机制时，必须配置加密套件。

WEP 加密套件只能配置 WEP40/WEP104/WEP128 其中的一种，且需要配置与加密套件种类相对应的 WEP 密钥及 WEP 密钥 ID。

WEP128 和 CCMP 或 TKIP 不能同时配置。

【举例】

配置在帧加密时使用 TKIP 加密套件。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] cipher-suite tkip
```

【相关命令】

- **security-ie**
- **wep key**

- **wep key-id**

1.1.3 gtk-rekey client-offline enable

gtk-rekey client-offline enable 命令用来开启客户端离线更新 GTK 功能。

undo gtk-rekey client-offline enable 命令用来关闭客户端离线更新 GTK 功能。

【命令】

gtk-rekey client-offline enable

undo gtk-rekey client-offline enable

【缺省情况】

客户端离线更新 GTK 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】

只有开启了更新 GTK 功能，客户端离线更新 GTK 的功能才能生效。

【举例】

开启客户端离线更新 GTK 功能。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] gtk-rekey client-offline enable
```

【相关命令】

- **gtk-rekey enable**

1.1.4 gtk-rekey enable

gtk-rekey enable 命令用来开启更新 GTK 功能。

undo gtk-rekey enable 命令用来关闭更新 GTK 功能。

【命令】

gtk-rekey enable

undo gtk-rekey enable

【缺省情况】

更新 GTK 功能处于开启状态。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【举例】

开启更新 GTK 功能。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] gtk-rekey enable
```

1.1.5 gtk-rekey method

gtk-rekey method 命令用来配置 GTK 更新方法。

undo gtk-rekey method 命令用来恢复缺省情况。

【命令】

gtk-rekey method { **packet-based** [*packet*] | **time-based** [*time*] }

undo gtk-rekey method

【缺省情况】

GTK 更新采用基于时间的方法，时间间隔为 86400 秒。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

packet-based：表示基于数据包的更新方法。

packet：指定传输的数据包（包括组播和广播）的数目，在传送指定数目的数据包（包括组播和广播）后更新 GTK，取值范围为 5000～4294967295，缺省值为 10000000。

time-based：表示基于时间的 GTK 更新方法。

time：指定 GTK 密钥更新的周期。取值范围为 180～604800，单位为秒，缺省值为 86400 秒。

【使用指导】

只有开启了 GTK 更新功能，GTK 更新方法才能生效。

使用该命令配置 GTK 密钥更新方法，多次执行本命令，最后一次执行的命令生效。例如，如果先配置了基于数据包的方法，然后又配置了基于时间的方法，则最后生效的是基于时间的方法。

若该命令在无线服务模板处于开启状态下配置，则分为以下几种情况：

- 基于时间的 GTK 的更新方式不改变，只改变时间值，则在原有定时器超时之后，新的定时器才可以生效；
- 基于报文数的 GTK 更新方式不改变，只改变报文数值，则该新的配置立即生效；
- 更新方式由基于时间更新改为基于报文数更新，则删除 GTK 更新定时器，在组播或广播报文数大于配置的数目值之后立即生效；
- 更新方式由基于报文数更新改为基于时间更新，则基于时间方式立即生效。

【举例】

配置基于时间的 GTK 更新方法。

```
<Sysname> system-view
```

```
[Sysname] wlan service-template security
[Sysname-wlan-st-security] gtk-rekey method time-based 3600
```

配置基于数据包的 GTK 更新方法。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] gtk-rekey method packet-based 600000
```

【相关命令】

- **gtk-rekey enable**

1.1.6 key-derivation

key-derivation 命令用来配置密钥衍生算法。

undo key-derivation 命令用来恢复缺省情况。

【命令】

key-derivation { **sha1** | **sha1-and-sha256** | **sha256** }

undo key-derivation

【缺省情况】

密钥衍生算法为 **sha1**。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

sha1：表示 SHA1 算法，它使用 HMAC-SHA1 算法进行迭代计算产生密钥。

sha1-and-sha256：表示 SHA1 和 SHA256 算法，它使用 HMAC-SHA1 或 HMAC-SHA256 算法进行迭代计算产生密钥。

sha256：表示 SHA256 算法，它使用 HMAC-SHA256 算法进行迭代计算产生密钥。

【使用指导】

当使用 RSNA 安全机制，密钥衍生算法才会生效。

如果配置保护管理帧功能为 **mandatory** 模式，建议指定密钥衍生类型为 **sha256**。

本命令只能在无线服务模板处于关闭状态时配置。

【举例】

配置密钥衍生算法为 SHA256。

```
<Sysname> system-view
[Sysname] wlan service-template 1
[Sysname-wlan-st-1] key-derivation sha256
```

【相关命令】

- **akm mode**
- **cipher-suite**

- **security-ie**

1.1.7 pmf

pmf 命令用来开启保护管理帧功能。

undo pmf 命令用来关闭保护管理帧功能。

【命令】

pmf { **mandatory** | **optional** }

undo pmf

【缺省情况】

保护管理帧功能处于关闭状态。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

mandatory：指定保护管理帧功能为强制模式，即不支持保护管理帧功能的客户端无法接入。

optional：指定保护管理帧功能为可选模式，即支持或不支持保护管理帧功能的客户端均可接入。

【使用指导】

当使用 RSNA 安全机制且配置了 CCMP 加密套件和 RSN 安全信息元素时，保护管理帧功能才会生效。

【举例】

开启保护管理帧功能。

```
<Sysname> system-view
[Sysname] wlan service-template 1
[Sysname-wlan-st-1] pmf optional
```

【相关命令】

- **security-ie**
- **cipher-suite**

1.1.8 pmf association-comeback

pmf association-comeback 命令用来配置保护管理帧的关联返回时间。

undo pmf association-comeback 命令用来恢复缺省情况。

【命令】

pmf association-comeback *time*

undo pmf association-comeback

【缺省情况】

保护管理帧的关联返回时间为 1 秒。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

time：保护管理帧的关联返回时间，取值范围为 1～20，单位为秒。

【使用指导】

如果 AP 拒绝客户端的关联/重关联请求帧，会向客户端发送关联/重关联响应帧，其中携带了保护管理帧关联返回时间。到了保护管理帧关联返回时间，AP 才会接收客户端的关联/重关联请求帧。

【举例】

配置保护管理帧的关联返回时间为 2 秒。

```
<Sysname> system-view
[Sysname] wlan service-template 1
[Sysname-wlan-st-1] pmf association-comeback 2
```

1.1.9 pmf saquery retrycount

pmf saquery retrycount 命令用来配置 AP 发送 SA Query request 的最大重传次数。

undo pmf saquery retrycount 命令用来恢复缺省情况。

【命令】

pmf saquery retrycount *count*

undo pmf saquery retrycount

【缺省情况】

AP 发送 SA Query request 帧的最大重传次数为 4 次。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

count：表示 AP 发送 SA Query request 帧的最大重传次数，取值范围为 1～16。

【使用指导】

若 AP 在 SA Query 重试次数内未收到 SA Query 响应帧，并且关联返回时间已经超时，则 AP 将认为客户端已经掉线。

【举例】

设置 AP 发送 SA Query request 帧的最大重传次数为 3。

```
<Sysname> system-view
[Sysname] wlan service-template 1
[Sysname-wlan-st-1] pmf saquery retrycount 3
```

【相关命令】

- **pmf**
- **pmf saquery retrycount**

1.1.10 pmf saquery retrytimeout

pmf saquery retrytimeout 命令用来设置 AP 发送 SA Query request 帧的时间间隔。

undo pmf saquery retrytimeout 命令用来恢复缺省情况。

【命令】

pmf saquery retrytimeout *timeout*

undo pmf saquery retrytimeout

【缺省情况】

AP 发送 SA Query request 帧的时间间隔为 200 毫秒。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

timeout：指定 AP 发送 SA Query request 帧的时间间隔，取值范围为 100～500，单位为毫秒。

【举例】

设置 AP 发送 SA Query request 帧的时间间隔为 300 毫秒。

```
<Sysname> system-view
[Sysname] wlan service-template 1
[Sysname-wlan-st-1] pmf saquery retrytimeout 300
```

【相关命令】

- **pmf**
- **pmf saquery retrytimeout**

1.1.11 preshared-key

preshared-key 命令用来配置 PSK 密钥。

undo preshared-key 命令用来恢复缺省情况。

【命令】

preshared-key { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*

undo preshared-key

【缺省情况】

未配置 PSK 密钥。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

pass-phrase：以字符串方式输入预共享密钥。

raw-key：以十六进制数方式输入预共享密钥。

cipher：以密文方式设置密钥。

simple：以明文方式设置密钥，该密钥将以密文形式存储。

string：密钥字符串，区分大小写。密钥长度的范围与选择的密钥参数有关，具体关系如下：

- 对于 **pass-phrase**，明文密钥为 8～63 个字符的字符串，密文密钥为 8～117 个字符的字符串。
- 对于 **raw-key**，明文密钥为 64 个十六进制数，密文密钥为 8～117 个字符的字符串。

【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。只有认证密钥管理模式为 PSK 时，此命令才能够生效，当认证密钥管理模式为 802.1X 时，配置了此项，无线服务模板可以使能，但此配置不会生效。

PSK 密钥只能配置一个。

【举例】

配置使用明文字符串 12345678 作为 PSK 密钥。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] akm mode psk
[Sysname-wlan-st-security] preshared-key pass-phrase simple 12345678
```

【相关命令】

- **akm mode**

1.1.12 ptk-lifetime

ptk-lifetime 命令用来配置 PTK 的生存时间。

undo ptk-lifetime 命令用来恢复缺省情况。

【命令】

ptk-lifetime *time*

undo ptk-lifetime

【缺省情况】

PTK 的生存时间为 43200 秒。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

time：指定生存时间，取值范围为 180～604800，单位为秒。

【使用指导】

若该命令在无线服务模板处于开启状态下配置，则在原有定时器超时后，该配置生效。

【举例】

配置 PTK 生存时间为 200 秒。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] ptk-lifetime 200
```

1.1.13 ptk-rekey enable

ptk-rekey enable 命令用来开启 PTK 更新功能。

undo ptk-rekey enable 命令用来关闭 PTK 更新功能。

【命令】

ptk-rekey enable

undo ptk-rekey enable

【缺省情况】

PTK 更新功能处于开启状态。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【使用指导】

PTK 更新是对单播数据报文的加密密钥进行更新的一种安全手段，采用重新进行四次握手协商出新的 PTK 密钥的更新机制。

开启本功能后，设备会按照 **ptk-lifetime** 命令配置的生存时间周期性的更新 PTK。

【举例】

开启 PTK 更新功能。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] ptk-rekey enable
```

【相关命令】

- **ptk-lifetime**

1.1.14 security-ie

security-ie 命令用来配置信标和探查响应帧携带安全 IE。

undo security-ie 命令用来配置信标和探查响应帧不携带指定的安全 IE。

【命令】

security-ie { **rsn** | **wpa** } *

undo security-ie { **rsn** | **wpa** } *

【缺省情况】

信标和探查响应帧不携带 WPA IE、RSN IE 或 OSEN IE。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

rsn：设置在 AP 发送信标和探查响应帧时携带 RSN IE。RSN IE 通告了 AP 的 RSN 能力。

wpa：设置在 AP 发送信标和探查响应帧时携带 WPA IE。WPA IE 通告了 AP 的 WPA 能力。

【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，并且必须要配置 CCMP 或 TKIP 加密套件。

当 WLAN 网络采用 RSNA 安全机制时，必须配置安全 IE。

【举例】

配置信标帧和探查响应帧携带 RSN 信息元素。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] security-ie rsn
```

【相关命令】

- **akm mode**
- **cipher-suite**

1.1.15 snmp-agent trap enable wlan usersec

snmp-agent trap enable wlan usersec 命令用来开启用户安全的告警功能。

undo snmp-agent trap enable wlan usersec 命令用来关闭用户安全的告警功能。

【命令】

snmp-agent trap enable wlan usersec

undo snmp-agent trap enable wlan usersec

【缺省情况】

用户安全的告警功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启了告警功能之后，该模块会生成告警信息，用于报告该模块的重要事件。生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。（有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。）

【举例】

开启用户安全的告警功能。

```
<Sysname> system-view
[Sysname] snmp-agent trap enable wlan usersec
```

1.1.16 tkip-cm-time

tkip-cm-time 命令用来配置发起 TKIP 反制策略时间。

undo tkip-cm-time 命令用来恢复缺省情况。

【命令】

tkip-cm-time *time*

undo tkip-cm-time

【缺省情况】

发起 TKIP 反制策略时间为 0，即不启动反制策略。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

time：设置发起 TKIP 反制策略时间，取值范围为 0～3600，单位为秒。

【使用指导】

启动 TKIP 反制策略后，如果相邻两次 MIC 错误的时间间隔小于等于配置的时间，则会解除所有关联到该无线服务的客户端，并且只有在 TKIP 反制策略实施的时间（60 秒）后，才允许客户端重新建立关联。

只有在配置了 TKIP 加密套件时，此命令才能够生效。

若该命令在无线服务模板处于开启状态时配置，则原有定时器超时后，该配置生效。

【举例】

配置发起 TKIP 反制策略时间为 180 秒。

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

```
[Sysname-wlan-st-security] tkip-cm-time 180
```

【相关命令】

- **cipher-suite**

1.1.17 wep key

wep key 命令用来配置 WEP 密钥。

undo wep key 命令用来删除指定的 WEP 密钥。

【命令】

wep key *key-id* { **wep40** | **wep104** | **wep128** } { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*

undo wep key *key-id*

【缺省情况】

未配置 WEP 密钥。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

key-id：密钥的 ID，取值范围为 1～4。

wep40：设置 WEP40 密钥选项。

wep104：设置 WEP104 密钥选项。

wep128：设置 WEP128 密钥选项。

pass-phrase：表示共享密钥为字符串。

raw-key：表示共享密钥为十六进制数。

cipher：以密文方式设置密钥。

simple：以明文方式设置密钥，该密钥将以密文形式存储。

string：密钥字符串，区分大小写。明文密钥的长度范围和选择的密钥参数有关，具体关系如下。密文密钥为 37～73 个字符的字符串。

- 对于 **wep40 pass-phrase**，明文密钥为 5 个字符的字符串。
- 对于 **wep104 pass-phrase**，明文密钥为 13 个字符的字符串。
- 对于 **wep128 pass-phrase**，明文密钥为 16 个字符的字符串。
- 对于 **wep40 raw-key**，明文密钥为 10 个 16 进制数。
- 对于 **wep104 raw-key**，明文密钥为 26 个 16 进制数。
- 对于 **wep128 raw-key**，明文密钥为 32 个 16 进制数。

【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。

WEP 密钥只有在配置了 WEP 加密套件的前提下才生效，最多可以配置四个 WEP 密钥。

【举例】

配置加密套件为 WEP40，并配置 WEP40 密钥为明文 12345。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] wep key 1 wep40 pass-phrase simple 12345
```

【相关命令】

- **cipher-suite**
- **wep key-id**

1.1.18 wep key-id

wep key-id 命令用来选用 WEP 密钥。

undo wep key-id 命令用来恢复缺省情况。

【命令】

wep key-id { **1** | **2** | **3** | **4** }

undo wep key-id

【缺省情况】

WEP 加密使用的密钥 ID 为 1。

【视图】

无线服务模板视图

【缺省用户角色】

network-admin

【参数】

1：选择密钥 ID 为 1。

2：选择密钥 ID 为 2。

3：选择密钥 ID 为 3。

4：选择密钥 ID 为 4。

【使用指导】

如果使用 RSNA 安全机制，密钥 ID 不能为 1，需要配置其它密钥索引值。因为 RSN 和 WPA 协商的密钥 ID 将为 1。本命令只能在无线服务模板处于关闭状态时配置。

只有在配置了与密钥长度相对应的 WEP 加密套件时，指定 ID 的密钥才会生效。

当配置了多个密钥，可以通过配置密钥 ID 选择要使用的加密密钥。

【举例】

配置 WEP40 加密套件，WEP40 密钥为明文 12345，配置密钥 ID 为 1。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] cipher-suite wep40
[Sysname-wlan-st-security] wep key 1 wep40 pass-phrase simple 12345
[Sysname-wlan-st-security] wep key-id 1
```

【相关命令】

- **wep key**

1.1.19 wep mode dynamic

wep mode dynamic 命令用来开启动态 WEP 加密机制。

undo wep mode dynamic 命令用来关闭动态 WEP 加密机制。

【命令】

wep mode dynamic

undo wep mode dynamic

【缺省情况】

动态 WEP 加密机制处于关闭状态。

【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。

配置动态 WEP 加密必须和 dot1x 用户接入认证模式一起使用，并且 **wep key-id** 不能配置为 4。

【举例】

开启动态 WEP 加密机制。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] wep mode dynamic
```

【相关命令】

- **cipher-suite**
- **client-security authentication-mode**（用户接入与认证命令参考-WLAN 用户接入认证）
- **wep key**
- **wep key-id**

1.1.20 wlan password-failure-limit enable

wlan password-failure-limit enable 命令用来开启密码错误限制功能。

undo wlan password-failure-limit enable 命令用来关闭密码错误限制功能。

【命令】

wlan password-failure-limit enable [**detection-period** *detection-period*] [**failure-threshold** *failure-threshold*]

undo wlan password-failure-limit enable

【缺省情况】

密码错误限制功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

detection-period *detection-period*：指定密码错误限制功能的检测周期，取值范围是 5～600，单位为秒，缺省值为 100。

failure-threshold *failure-threshold*：指定密码错误限制功能的检测阈值，取值范围是 1～100，缺省值为 20。

【使用指导】

开启本功能后，在指定检测周期内密码校验失败次数达到指定上限时，客户端会被立即加入到动态黑名单中。有关动态黑名单的详细介绍请参见“WLAN 配置指导”中的“WLAN 接入”。

只有当身份认证与密钥管理模式为 PSK 或者 Private-PSK 时，密码错误限制功能才会生效。

本功能仅对在设备上进行关联的新接入的无线客户端生效。

当 STAMGR 进程重启（例如：设备重启导致的 STAMGR 进程重启）后，本功能将对密码校验失败次数重新进行计数。

本功能不支持 IRF 组网中 AP 直接从备份 AC 上线的情况。

【举例】

配置无线客户端的密码错误限制检测周期为 300 秒，检测阈值为 50 次。

```
<Sysname> system-view
[Sysname] wlan password-failure-limit enable detection-period 300 failure-threshold 50
```