目 录

1 WLAN用户安全配置

1.1 WLAN用户安全简介

最初 802.11 的安全机制被称为 Pre-RSNA 安全机制，它的认证机制不完善，容易被攻破，存在安全隐患，且在 WEP 加密机制中，由于连接同一 BSS 下的所有客户端都使用同一加密密钥和 AP 进行通信，一旦某个用户的密钥泄露，那么所有用户的数据都可能被窃听或篡改，所以 IEEE 制订了 802.11i 协议来加强无线网络的安全性。

但 802.11i 仅对无线网络的数据报文进行加密保护，而不对管理帧进行保护，所以管理帧的机密性、真实性、完整性无法保证，容易受到仿冒或监听，例如：恶意攻击者通过获取设备的 MAC 地址并仿冒设备恶意拒绝客户端认证或恶意结束设备与客户端的关联。802.11w 无线加密标准建立在 802.11i 框架上，通过保护无线网络的管理帧来解决上述问题，进一步增强无线网络的安全性。

1.2 Pre-RSNA安全机制

Pre-RSNA 安全机制采用开放式系统认证（Open system authentication）和共享密钥认证（Shared key authentication）两种认证模式来进行客户端认证，并且采用 WEP 加密方式对数据进行加密来保护数据机密性，以对抗窃听。WEP 加密使用 RC4 加密算法（一种流加密算法）实现数据报文的加密，WEP 加密支持 WEP40、WEP104 和 WEP128 三种密钥长度。

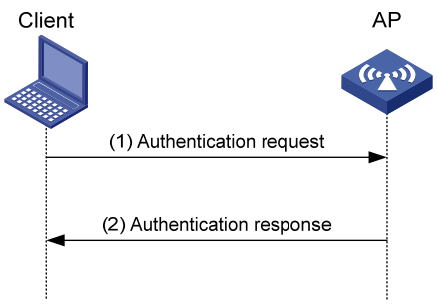
1.2.1 开放系统认证

开放系统认证（Open system authentication）是缺省使用的认证方式，也是最简单的认证算法，即不认证。如果认证类型设置为开放系统认证，则所有请求认证的客户端都会通过认证。开放系统认证包括两个步骤，如 图 1-1 所示：

(1) 客户端向 AP 发起认证请求；

(2) AP 确定客户端可以通过无线链路认证，并向客户端回应认证结果为“成功”。

图1-1 开放系统认证过程



1.2.2 共享密钥认证

共享密钥认证（Shared key authentication）需要客户端和 AP 配置相同的 WEP 密钥。

共享密钥认证的认证过程如 图 1-2 所示：

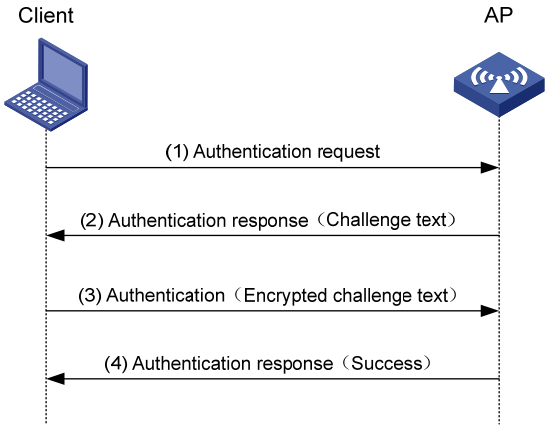
(1) 客户端先向 AP 发送认证请求；

(2) AP 会随机产生一个 Challenge Text（即一个字符串）发送给客户端；

(3) 客户端使用 WEP 密钥将接收到的 Challenge Text 加密后再发送给 AP；

(4) AP 使用 WEP 密钥解密接收到的消息，并对解密后的字符串和原始字符串进行比较。如果相同，则说明客户端通过了链路层认证，否则链路层认证失败。

图1-2 共享密钥认证过程



1.3 RSNA安全机制

802.11i 安全机制又被称为 RSNA（Robust Security Network Association，健壮安全网络连接）安全机制，包括 WPA（Wi-Fi Protected Access，Wi-Fi 保护访问）和 RSN（Robust Security Network，健壮安全网络）两种安全模式，采用 AKM（Authentication and Key Management，身份认证与密钥管理）对用户身份的合法性进行认证，对密钥的生成、更新进行动态管理，并且采用 TKIP（Temporal Key Integrity Protocol，临时密钥完整性协议）和 CCMP（Counter mode with CBC-MAC Protocol，[计数器模式]搭配[区块密码锁链一信息真实性检查码]协议）加密机制对报文进行加密。

AKM 分为 802.1X、Private-PSK 和 PSK 和三种模式：

- 802.1X：采用 802.1X 认证对用户进行身份认证，并在认证过程中生成 PMK（Pairwise Master Key，成对主密钥），客户端和 AP 使用该 PMK 生成 PTK（Pairwise Transient Key，成对临时密钥）。
- Private-PSK：采用 PSK（Pre-Shared Key，预共享密钥）认证进行身份认证，使用客户端的 MAC 地址作为 PSK 密钥生成 PMK，客户端和 AP 使用该 PMK 生成 PTK。
- PSK：采用 PSK 认证进行身份认证，并通过 PSK 密钥生成 PMK，客户端和 AP 使用该 PMK 生成 PTK。

说明

当 WLAN 网络采用 RSNA 安全机制时，链路层认证将协商为开放系统认证。

1.3.1 身份认证

802.11i 协议规定使用两种身份认证方式，以下分别介绍：

- 对于安全要求标准较高的企业、政府等机构，推荐使用认证服务器通过 802.1X 认证方式对客户端进行身份认证。有关 802.1X 认证的详细介绍及相关配置，请参见“WLAN 配置指导”中的“WLAN 用户接入认证”。
- 对于安全要求标准较低的家庭用户等，推荐使用 PSK 方式对客户端进行认证。PSK 认证方式需要在 AP 侧预先输入预共享密钥，在客户端关联过程中，手动输入该密钥，AP 和客户端通过四次握手密钥协商来验证客户端的预共享密钥的合法性，若 PTK 协商成功，则证明该用户合法，以此来达到认证的目的。

1.3.2 密钥管理

密钥用于对数据进行加密来提高 WLAN 网络的安全性。密钥管理机制定义了密钥的生成和密钥的更新等一系列的过程，以此来确保每个用户使用安全的密钥。

1. 密钥种类

802.11i 协议中密钥主要包括 PTK 和 GTK（Group Temporal Key，群组临时密钥）两种，以下分别介绍。

(1) PTK

PTK用于保护单播数据，PTK结构如 图 1-3 所示。

图1-3 PTK 结构图

- KCK（EAPOL-Key Confirmation Key，确认密钥）：用来校验 EAPOL-Key 帧的完整性。
- KEK（EAPOL-Key Encryption Key，加密密钥）：用来加密 EAPOL-Key 帧中的 Key Data 字段。
- TK（Temporal Key，临时密钥）：用来对单播数据报文进行加密的密钥。

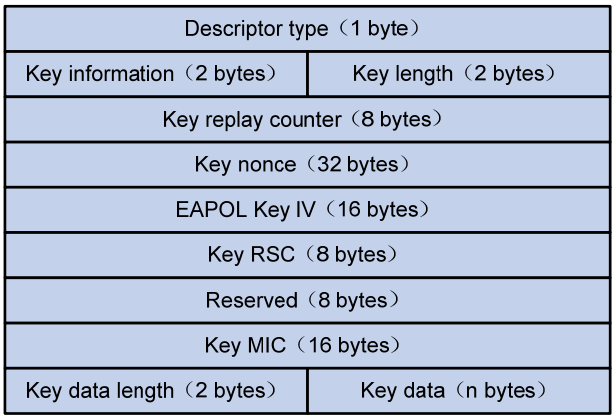
(2) GTK

GTK 用于保护组播和广播数据。GTK 的结构包含 TK 和其它字段，其中 TK 是用来对组播和广播数据进行加密的密钥。

2. EAPOL-Key报文格式

802.11i协议规定密钥协商过程使用的报文为EAPOL-Key数据报文，报文格式如 图 1-4 所示。

图1-4 EAPOL-Key 报文格式



EAPOL-Key报文的各字段含义如 表 1-1 所示。

表1-1 EAPOL-Key 报文字段含义

字段	含义
Descriptor type	表示网络类型是WPA网络或RSN网络
Key information	有关Key information的详细介绍，请参见“表1-2Key information字段含义”
Key length	表示密钥的长度
Key replay counter	此字段表示AP发送的EAPOL-Key报文的个数，即AP每发送一个EAPOL-Key报文该字段都会加1，目的是防止重放攻击。在开始密钥协商时，AP发送的EAPOL-Key报文中该字段为0，客户端接收到EAPOL-Key报文，将此位记录到本地，当客户端再次接收到AP发送的EAPOL-Key报文时，报文内的该字段必须要大于本地所记录的，否则丢弃该报文等待重传。当AP端接收到客户端的报文时，此字段必须和AP本地保存的相同，否则等待重传，直到接收到合法的Key replay counter。若达到最大重传次数时，AP会将客户端删除
Key nonce	该字段用来传递生成PTK所用的随机值
EAPOL Key IV	该字段用于TKIP加密，只有加密方式为非CCMP时，该字段才被赋值
Key RSC	此字段表示AP发送的组播报文或广播报文的个数，即AP每发送一个组播或广播报文该字段都会加1，与Key replay counter字段的防止重放攻击作用相同
Reserved	保留字段
Key MIC	表示EAPOL-Key报文MIC（Message Integrity Check，信息完整性校验）值
Key data length	表示Key data字段长度
Key data	该字段要存放AP和客户端进行交互的数据，例如：GTK、PMKID（Pairwise Master key identifier，成对主密钥标识符，供漫游所用）等

Key information字段格式如 图 1-5 所示，各字段含义如 表 1-2 所示。

图1-5 Key information 字段格式

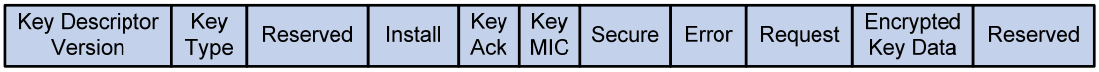


表1-2 Key information 字段含义

字段	含义
Key Descriptor Version	密钥版本位，长度为3比特，取值为1表示非CCMP密钥，取值为2表示CCMP密钥
Key Type	密钥类型位，长度为1比特，取值为1表示在进行单播密钥协商，取值为0表示在进行组播密钥协商
Reserved	保留位，长度为2比特，发送方将该位置为0，接收方忽略该值

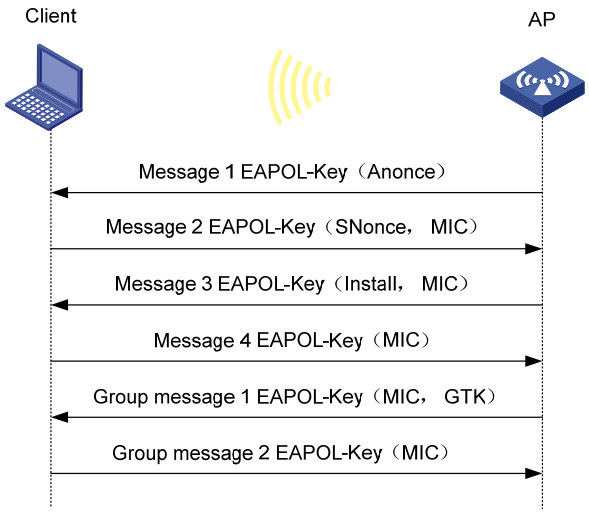
Install	安装密钥标记位，长度为1比特
	• 若 Key Type 位为 1：
	  ○ 安装密钥标记位为 1，表示客户端进行 TK 密钥安装
	  ○ 安装密钥标记位为 0，表示客户端不进行 TK 密钥安装
	• 若 Key Type 位为 0：
	则在发送方会将安装密钥标记位置为0，接收方忽略该位

Key Ack	密钥确认位，长度为1比特，取值为1表示AP期待客户端回复应答报文
Key MIC	信息完整性校验位，长度1比特，取值为1表示已经计算出MIC，并且将产生的MIC填充到EAPOL-Key报文的Key MIC字段中
Secure	安全位，长度为1比特，取值为1表示密钥已产生
Error	错误位，长度为1比特，取值为1表示客户端MIC校验失败；当且仅当Request位为1时，客户端才将该位置为1
Request	请求位，长度为1比特，由MIC校验失败的客户端发起，用来请求AP发起四次握手或者组播握手
Encrypted Key Data	加密密钥数据位，长度为1比特，取值为1表示Key data字段为加密数据
Reserved	保留位，长度为3比特，发送方将该位置位0，接收方忽略该值

3. WPA安全模式密钥协商过程

WPA是一种比WEP加密性能更强的安全机制。在 802.11i协议完善前，采用WPA为用户提供一个临时性的WLAN安全增强解决方案。在WPA安全网络中，客户端和AP通过使用EAPOL-Key报文进行四次握手协商出PTK，通过使用EAPOL-Key报文进行二次组播握手协商出GTK。协商过程如 图 1-6 所示。

图1-6 WPA 密钥协商过程



(1) AP 向客户端发送携带有随机数 ANonce 的第一个 EAPOL-Key 报文 Message 1；

(2) 客户端接收到报文 Message 1，使用 AP 端发送的随机数 ANonce、客户端的随机数 SNonce 和身份认证产生的 PMK 通过密钥衍生算法生成 PTK，并用 PTK 中的 KCK 产生 MIC（Message Integrity Check，信息完整性校验），并将 MIC 填充到 Message 2 报文中，然后向 AP 发送携带 SNonce 和 MIC 的第二个 EAPOL-Key 报文 Message 2；

(3) AP 接收到报文 Message 2，使用 SNonce、ANonce 和身份认证产生的 PMK 通过密钥衍生算法生成 PTK，并用 PTK 中的 KCK 生成 MIC，然后对 Message 2 报文做 MIC 校验，用 AP 端生成的 MIC 和报文中 MIC 进行比较，若两个 MIC 相同则说明 MIC 校验成功，否则校验失败。MIC 校验成功后，AP 向客户端发送携带通知客户端安装 PTK 标记和 MIC 的第三个 EAPOL-Key 报文 Message 3；

(4) 客户端接收到报文 Message 3，首先对报文进行 MIC 校验，校验成功后，安装单播密钥 TK，然后向 AP 发送携带 MIC 的第四个 EAPOL-Key 报文 Message 4；

(5) AP 接收到报文 Message 4，首先对报文进行 MIC 校验，若校验成功，则 AP 安装单播密钥 TK，密钥安装成功后 AP 使用随机值 GMK（Group Master Key，组播主密钥）和 AP 的 MAC 地址通过密钥衍生算法产生 GTK，并向客户端发送携带 MIC 和 GTK 的第五个 EAPOL-Key 报文 Group message 1；

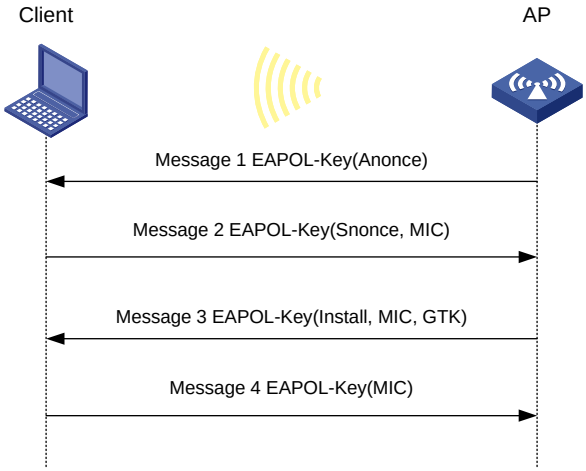
(6) 客户端接收到 Group message 1，首先对报文进行 MIC 校验，校验成功后安装组播密钥 TK，并向 AP 发送携带 MIC 的第六个 EAPOL-Key 报文 Group message 2；

(7) AP 接收到 Group message 2，首先对报文进行 MIC 校验，校验成功后安装组播密钥 TK。

4. RSN安全模式密钥协商过程

RSN是按照 802.11i协议为用户提供的一种WLAN安全解决方案。在RSN网络中，客户端和AP通过使用EAPOL-Key类型报文进行四次握手协商出PTK和GTK。协商过程如 图 1-7 所示。

图1-7 RSN 密钥协商过程



(1) AP 向客户端发送携带有随机数 ANonce 的第一个 EAPOL-Key 报文 Message 1；

(2) 客户端接收到报文 Message 1，使用 AP 端发送的随机数 ANonce、客户端的随机数 SNonce 和身份认证产生的 PMK 通过密钥衍生算法生成 PTK，并用 PTK 中的 KCK 产生 MIC，并填充到 Message 2 报文中，然后向 AP 发送携带 SNonce 和 MIC 的第二个 EAPOL-Key 报文 Message 2；

(3) AP 接收到报文 Message 2，使用 SNonce、ANonce 和身份认证产生的 PMK 通过密钥衍生算法生成 PTK，并用 PTK 中的 KCK 生成 MIC，然后对 Message 2 报文做 MIC 校验，用 AP 端生成的 MIC 和报文中 MIC 进行比较，两个 MIC 相同则说明 MIC 校验成功，否则失败。MIC 校验成功后通过随机值 GMK 和 AP 的 MAC 地址通过密钥衍生算法产生 GTK，并向客户端发送携带通知客户端安装密钥标记、MIC 和 GTK 的第三个 EAPOL-Key 报文 Message 3；

(4) 客户端接收到报文 Message 3，首先对报文进行 MIC 校验，校验成功后客户端安装单播密钥 TK 和组播密钥 TK，然后向 AP 发送携带 MIC 的第四个 EAPOL-Key 报文 Message 4；

(5) AP 接收到报文 Message 4，首先对报文进行 MIC 校验，校验成功后安装密钥单播密钥 TK 和组播密钥 TK。

5. 密钥更新

如果客户端长时间使用一个密钥，或携带当前网络正在使用的组播密钥离线，此时网络被破坏的可能性很大，安全性就会大大降低。WLAN 网络通过身份认证与密钥管理中的密钥更新机制来提高 WLAN 网络安全性。密钥更新包括 PTK 更新和 GTK 更新。

- PTK 更新：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，来提高安全性。
- GTK 更新：GTK 更新是对组播数据报文的加密密钥进行更新的一种安全手段，采用重新进行两次组播握手协商出新的 GTK 密钥的更新机制，来提高安全性。

1.3.3 加密套件

由于 WEP 加密易破解，一旦攻击者收集到足够多的有效数据帧进行统计分析，那么将会造成数据泄露，无线网络将不再安全。802.11i 增加了 TKIP 和 CCMP 两种加密套件来保护用户数据安全，以下分别介绍。

1. TKIP

TKIP 加密机制依然使用 RC4 算法，所以不需要升级原来无线设备的硬件，只需通过软件升级的方式就可以提高无线网络的安全性。相比 WEP 加密机制，TKIP 有如下改进：

- 通过增长了算法的 IV（Initialization Vector，初始化向量）长度提高了加密的安全性。相比 WEP 算法，TKIP 直接使用 128 位密钥的 RC4 加密算法，而且将初始化向量的长度由 24 位加长到 48 位；
- 采用和 WEP 一样的 RC4 加密算法，但其动态密钥的特性很难被攻破，并且 TKIP 支持密钥更新机制，能够及时提供新的加密密钥，防止由于密钥重用带来的安全隐患；
- 支持 TKIP 反制功能。当 TKIP 报文发生 MIC 错误时，数据可能已经被篡改，也就是无线网络很可能正在受到攻击。当在一段时间内连续接收到两个 MIC 错误的报文，AP 将会启动 TKIP 反制功能，此时，AP 将通过关闭一段时间无线服务的方式，实现对无线网络攻击的防御。

2. CCMP

CCMP 加密机制使用 AES（Advanced Encryption Standard，高级加密标准）加密算法的 CCM（Counter-Mode/CBC-MAC，区块密码锁链－信息真实性检查码）方法，CCMP 使得无线网络安全有了极大的提高。CCMP 包含了一套动态密钥协商和管理方法，每一个无线用户都会动态的协商一套密钥，而且密钥可以定时进行更新，进一步提供了 CCMP 加密机制的安全性。在加密处理过程中，CCMP 也会使用 48 位的 PN（Packet Number）机制，保证每一个加密报文都会使用不同的 PN，在一定程度上提高安全性。

1.4 保护管理帧功能

保护管理帧功能通过保护无线网络中的管理帧来完善无线网络的安全性。802.11w 保护的管理帧包括解除认证帧，解除关联帧和部分强壮 Action 帧。

对于单播管理帧，保护管理帧功能使用对数据帧加密的 PTK 对单播管理帧进行加密，保证单播管理帧的机密性、完整性以及提供重放保护。

对广播/组播管理帧，保护管理帧功能使用 BIP（Broadcast Integrity Protocol，广播完整性协议）保证广播/组播管理帧的完整性以及提供重放保护，实现防止客户端受到仿冒 AP 的攻击。

当 AP 与客户端协商结果为使用保护管理帧功能时，AP 将使用 SA Query（Security Association Query，安全关联询问）机制增强客户端的安全连接。SA Query 包括主动 SA Query 和被动 SA Query。

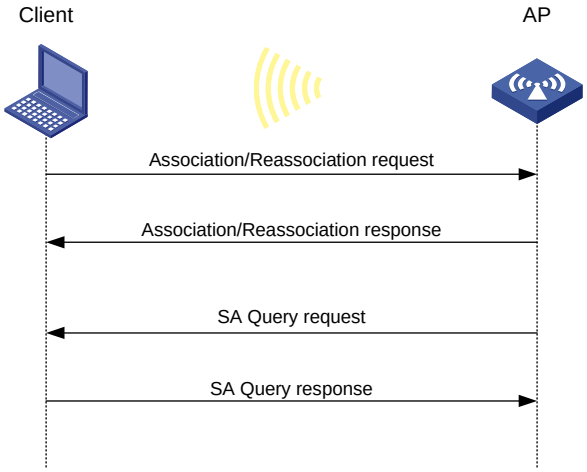
1.4.1 主动SA Query

在 AP 收到仿冒的关联/重关联请求帧的情况下，主动 SA Query 机制可以防止 AP 对客户端作出错误的响应。

当 AP 收到客户端的关联/重关联请求帧时，将发送关联/重关联响应帧，响应状态值为“关联/重关联临时被拒绝，稍后重连”，并携带通过 **pmf association-comeback** 命令指定关联返回时间，随后 AP 会触发 SA Query 过程。

AP 向客户端发送 SA Query 请求帧，若 AP 在 SA Query 超时时间内收到客户端发送的 SA Query 响应帧，则 AP 认为该客户端在线，当关联返回时间超时后，再次收到客户端的关联/重关联请求帧时，则会再次触发 SA Query 过程。若 AP 在 SA Query 超时时间内未收到客户端的 SA Query 响应帧，将再次触发 SA Query 请求帧。若 AP 在 SA Query 重试次数内收到 SA Query 响应帧，则认为客户端在线，当关联返回时间超时后，再次收到客户端的关联/重关联请求帧时，则会再次触发 SA Query 过程。若 AP 在 SA Query 重试次数内未收到 SA Query 响应帧，则 AP 将认为客户端已经掉线，当再次收到该客户端的关联/重关联请求帧时，允许其重新接入。若在关联返回时间内，SA Query 过程未完成，则当关联返回时间超时后，再次收到客户端的关联/重关联请求帧时，AP 将发送关联/重关联响应帧，响应状态值为“关联/重关联临时被拒绝，稍后重连”，并携带通过 **pmf association-comeback** 命令指定的关联返回时间，但不重新触发 SA Query 过程。

图1-8 主动 SA Query 过程

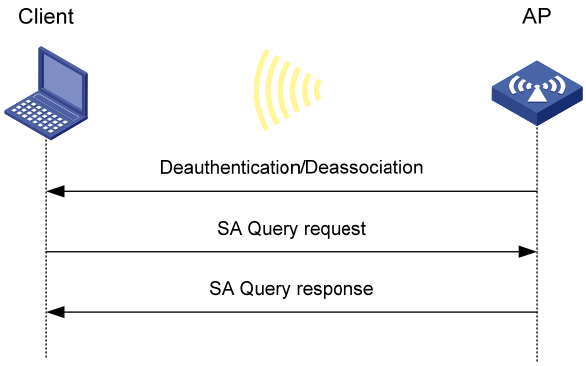


1.4.2 被动SA Query

在客户端收到未加密的解除关联/解除认证报文（失败码为 6 或 7）的情况下，被动 SA Query 机制可以防止客户端异常下线。

当客户端收到一个未保护的解除关联帧或者解除认证帧，客户端会触发 SA Query 过程。客户端向 AP 发送 SA Query 请求帧，AP 回复 SA Query 响应帧。客户端收到 SA Query 响应帧，判定 AP 在线，AP 和客户端之间的连接处于正常状态，则客户端不对收到的解除关联/解除认证报文进行处理。若客户端未收到 AP 回复的 SA Query 相应帧，则客户端断开与 AP 的连接。

图1-9 被动 SA Query 过程



1.5 动态WEP加密安全机制

说明

当 WLAN 网络采用动态 WEP 安全机制时，链路层认证将协商为开放系统认证。

在 Pre-RSNA 安全机制的 WEP 加密机制中，由于连接同一 BSS 下的所有客户端都使用同一加密密钥和 AP 进行通信，一旦某个用户的密钥泄露，那么所有用户的数据都可能被窃听或篡改，因此 802.11 提供了动态 WEP 加密机制。在动态 WEP 加密机制中，加密单播数据帧的 WEP 密钥是由客户端和认证服务器通过 802.1X 认证协商产生，保证了每个客户端使用不同的 WEP 单播密钥，从而提高了单播数据帧传输的安全性。组播密钥是 WEP 密钥，若未配置 WEP 密钥，则 AP 使用随机算法产生组播密钥。

当客户端通过 802.1X 认证后， AP 通过发送 RC4 EAPOL-Key 报文将组播密钥及密钥 ID 以及单播密钥的密钥 ID（固定为 4）分发给客户端。

1.6 协议规范

与用户安全相关的协议规范有：

- IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements－2004
- WI-FI Protected Access – Enhanced Security Implementation Based On IEEE P802.11i Standard-Aug 2004
- Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—802.11, 1999
- IEEE Standard for Local and metropolitan area networks ”Port-Based Network Access Control” 802.1X™-2004
- 802.11i IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements

- 802.11w IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements

1.7 WLAN用户安全配置任务简介

1. Pre-RSNA安全机制配置任务简介

使用 Pre-RSNA 安全机制，需要配置 WEP 加密套件及对应长度的 WEP 密钥，客户端上线时，客户端和 AP 根据客户端网卡的设置，协商链路层认证。

表1-3 Pre-RSNA 安全机制配置任务简介

配置任务	说明	详细配置
配置加密套件	必选	1.8.3
配置WEP密钥	必选	1.8.9
开启告警功能	可选	1.9

2. RSNA安全机制配置任务简介

使用 RSNA 安全机制，身份认证与密钥管理、安全信息元素、CCMP 或 TKIP 加密套件必须同时配置，且客户端网卡必须设置为开放式系统认证。

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

表1-4 RSNA 安全机制配置任务简介

配置任务	说明	详细配置
配置身份认证与密钥管理模式	必选	1.8.1
配置安全信息元素	必选	1.8.2
配置加密套件	必选	1.8.3
配置PSK密钥	可选	1.8.4
配置密钥衍生算法	可选	1.8.5
配置GTK更新功能	可选	1.8.6
配置PTK的生存时间	可选	1.8.7
配置TKIP反制时间	可选	1.8.8
配置WEP密钥	可选	1.8.9
配置保护管理帧功能	可选	1.8.10
开启告警功能	可选	1.9

3. 动态WEP加密机制配置任务简介

在使用动态 WEP 安全机制时，单播密钥是由客户端和认证服务器通过 802.1X 认证协商产生，因此必须配置用户接入认证模式为 dot1x 模式。

在开启动态 WEP 加密机制后：

- 若配置了 WEP 加密套件、加密套件对应的 WEP 密钥且指定了使用该 WEP 密钥的 ID，则以配置的加密套件对单播和组播报文加密，WEP 密钥作为组播密钥。客户端和认证服务器会协商与配置的 WEP 加密套件相对应的单播密钥。
- 若未配置 WEP 加密套件、WEP 密钥及密钥 ID，则使用加密套件 WEP104 对单播和组播报文进行加密，AP 会随机生成长度为 104 比特的字符串作为组播密钥，并且组播密钥 ID 为 1。系统会协商出 WEP104 密钥做为单播密钥。

表1-5 动态 WEP 加密机制配置任务简介

配置任务	说明	详细配置
配置加密套件	可选	1.8.3
配置WEP密钥	可选	1.8.9
开启动态WEP加密机制	必选	1.8.11
开启告警功能	可选	1.9

1.8 WLAN用户安全配置

1.8.1 配置身份认证与密钥管理模式

身份认证与密钥管理模式和 WLAN 用户接入认证的关系如下：

- 当用户选择 802.1X 身份认证与密钥管理时，WLAN 用户接入认证模式只能配置为 802.1X 模式；
- 当用户选择 Private-PSK 模式时，WLAN 用户接入认证模式只能配置为 MAC 地址认证模式；
- 当身份认证与密钥管理为 PSK 模式时，WLAN 用户接入认证模式只能使用 Bypass 认证或者 MAC 地址认证模式；
- 当用户选择 Wi-Fi 联盟匿名 802.1X 身份认证与密钥管理时，WLAN 用户接入认证模式只能配置为 802.1X 模式。

表1-6 配置身份认证与密钥管理模式

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置身份认证与密钥管理的模式	**akm mode** { **dot1x** | **private-psk** | **psk** | **anonymous-dot1x** }	缺省情况下，未配置身份认证与密钥管理模式

1.8.2 配置安全信息元素

安全信息元素对应的是当前设备所支持的网络类型，OSEN、WPA 或 RSN。用户如何配置取决于客户端所支持的网络类型。

表1-7 配置安全信息元素

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置安全信息元素	**security-ie** { **osen** | **rsn** | **wpa** }	缺省情况下，信标和探查响应帧不携带WPA IE、RSN IE或OSEN IE

1.8.3 配置加密套件

加密套件是对数据加密和解密的方法。加密套件如下：

- WEP40/WEP104/WEP128
- CCMP
- TKIP

WEP128 加密套件和 CCMP 或 TKIP 不能同时配置。

表1-8 配置加密套件

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置加密套件	**cipher-suite** { **ccmp** | **tkip** | **wep40** | **wep104** | **wep128** }	缺省情况下，未配置加密套件

1.8.4 配置PSK密钥

当身份认证与密钥管理为 PSK 模式时，则必须配置 PSK 密钥。当身份认证与密钥管理为 802.1X 模式时，若配置 PSK 密钥，则无线服务模板可以使能，但此配置不会生效。

表1-9 配置 PSK 密钥

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置PSK密钥	**preshared-key** { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*	缺省情况下，未配置PSK密钥

1.8.5 配置密钥衍生算法

当使用 RSNA 安全机制时，客户端和 AP 使用密钥衍生算法来产生 PTK/GTK。目前支持的散列算法有两种，分别是 SHA1 和 SHA256。SHA1 使用 HMAC-SHA1 算法进行迭代计算产生密钥，SHA256 使用 HMAC-SHA256 算法进行迭代计算产生密钥。SHA256 安全散列算法的安全性比 SHA1 安全散列算法安全性高。

表1-10 配置密钥衍生算法

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *stname*	-
配置密钥衍生算法	**key-derivation** { **sha1** | **sha256** | **sha1-and-sha256** }	缺省情况下，密钥衍生算法为sha1

1.8.6 配置GTK更新功能

若配置了身份认证与密钥管理、安全信息元素、TKIP 或 CCMP 加密套件，则系统将使用密钥协商来产生 GTK，此时可以配置 GTK 更新，触发 GTK 更新的方式有如下三种：

- 基于时间，在指定时间间隔后更新 GTK。
- 基于报文数，AP 发送了指定数目的广播或组播数据报文后更新 GTK。
- 客户端离线更新 GTK，当 BSS 中有客户端下线时，该 BSS 会更新 GTK。

表1-11 配置 GTK 更新功能

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
开启GTK更新功能	**gtk-rekey enable**	缺省情况下，GTK更新功能处于开启状态
配置GTK更新方法	**gtk-rekey method** { **packet-based** [*packet*] | **time-based** [*time*] }	缺省情况下，GTK更新采用基于时间的方法，时间间隔为86400秒 如果配置GTK更新方法为基于数据包的更新方法，缺省值为10000000
（可选）配置开启客户端离线GTK更新	**gtk-rekey client-offline enable**	缺省情况下，客户端离线更新GTK功能关闭

1.8.7 配置PTK的生存时间

若配置了身份认证与密钥管理、安全信息元素、TKIP 或 CCMP 加密套件，则系统将使用密钥协商来产生 PTK，此时可以设置 PTK 的生存时间，表明在指定的时间间隔后更新 PTK。

表1-12 配置 PTK 的生存时间

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置PTK的生存时间	**ptk-lifetime** *time*	缺省情况下，PTK的生存时间为43200秒

1.8.8 配置TKIP反制时间

若配置了 TKIP 加密套件，TKIP 可以通过配置反制时间的方式启动反制策略，来阻止黑客的攻击。

表1-13 配置 TKIP 反制时间

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置TKIP反制时间	**tkip-cm-time** *time*	缺省情况下，发起TKIP反制策略时间为0，即不启动反制策略

1.8.9 配置WEP密钥

若使用 RSNA 安全机制，且加密套件配置了 WEP40/WEP104/WEP128 和相对应长度的 WEP 密钥，则系统不会使用通过密钥协商产生的组播密钥为组播报文加密，而是选择安全性较弱的 WEP 的密钥做为组播密钥。

若使用 Pre-RSNA 安全机制，则客户端与 AP 将使用 WEP 密钥通过 WEP 加密方式对数据报文进行加密。

若使用动态 WEP 加密机制，则不能将 WEP 加密使用的密钥 ID 配置为 4。

表1-14 配置 WEP 密钥

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
配置WEP密钥	**wep key** *key-id* { **wep40** | **wep104** | **wep128** } { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*	缺省情况下，未配置WEP密钥
配置WEP加密使用的密钥ID	**wep key-id** { **1** | **2** | **3** | **4** }	缺省情况下，密钥ID为1

1.8.10 配置保护管理帧功能

配置保护管理帧功能有以下三种情况：

- 当保护管理帧功能关闭时，支持或不支持保护管理帧功能的客户端均可上线，但不对通信过程中的管理帧进行保护。
- 当保护管理帧功能为 **optional** 时，支持或不支持保护管理帧功能的客户端均可上线，但仅对支持保护管理帧功能上线客户端提供保护管理帧功能。
- 当保护管理帧为 **mandatory** 时，支持保护管理帧功能的客户端可上线，同时对通信过程中的管理帧进行保护，不支持保护管理帧功能的客户端无法上线。

要使用保护管理帧功能，必须使用 RSNA 安全机制，且加密套件必须配置为 CCMP 加密套件，安全信息元素必须配置为 RSN。

表1-15 配置保护管理帧功能

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
开启保护管理帧功能	**pmf** { **optional** | **mandatory** }	缺省情况下，保护管理帧功能处于关闭状态
配置AP发送SA Query超时时间	**pmf saquery retrytimeout** *timeout*	缺省情况下，AP发送SA Query request帧的时间间隔为200毫秒
配置AP发送SA Query request帧的最大重传次数	**pmf saquery retrycount** *count*	缺省情况下，AP发送SA Query request帧的最大重传次数为4次
配置保护管理帧的关联返回时间	**pmf association-comeback** *time*	缺省情况下，保护管理帧的关联返回时间为1秒

1.8.11 开启动态WEP加密机制

WLAN 用户接入认证模式必须配置为 dot1x 模式，动态 WEP 加密功能才会生效。

表1-16 开启动态 WEP 加密功能

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-name*	-
开启动态WEP加密机制	**wep mode dynamic**	缺省情况下，动态WEP加密机制处于关闭状态

1.9 开启告警功能

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”。）

表1-17 开启告警功能

操作	命令	说明
进入系统视图	**system-view**	-
开启用户安全的告警功能	**snmp-agent trap enable wlan usersec**	缺省情况下，用户安全的告警功能处于关闭状态

1.10 WLAN用户安全显示和维护

在完成上述配置后，在无线服务模版视图下执行 **display** 命令可以显示配置后的 WLAN 用户安全运行情况，通过查看显示信息验证配置效果。

display wlan service-template、**display wlan client** 命令的详细介绍，请参见“WLAN 命令参考”中的“WLAN 接入”。

表1-18 WLAN 用户安全显示和维护

操作	命令
显示无线服务模板信息	**display wlan service-template** [*service-template-name*] [**verbose**]
显示客户端的信息	**display wlan client** [**interface** *interface-type interface-number* | **mac-address** *mac-address* | **service-template** *service-template-name*] [**verbose**]

1.11 WLAN用户安全典型配置举例

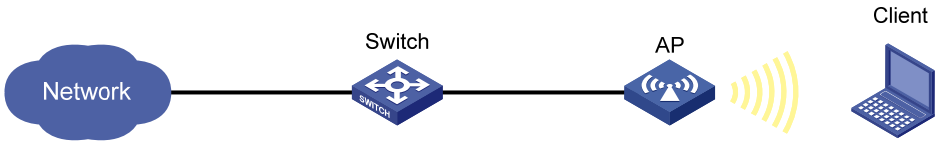
1.11.1 共享密钥认证配置举例

1. 组网需求

- 如 图 1-10 所示，Switch同时作为DHCP server为AP和Client分配IP地址。通过配置客户端在链路层使用WEP密钥 12345 接入无线网络。

2. 组网图

图1-10 共享密钥认证配置组网图



3. 配置步骤

(1) 创建无线服务模板

创建无线服务模板 service1 。

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

配置无线服务的 SSID 为 service。

```
[AP-wlan-st-service1] ssid service
```

(2) 配置 WEP 并使能无线服务模板

配置使用 WEP40 加密套件，配置密钥索引为 2，使用明文的字符串 12345 作为共享密钥。

```
[AP-wlan-st-service1] cipher-suite wep40
[AP-wlan-st-service1] wep key 2 wep40 pass-phrase simple 12345
[AP-wlan-st-service1] wep key-id 2
```

使能无线服务模板。

```
[AP-wlan-st-service1] service-template enable
[AP-wlan-st-service1] quit
```

(3) 将无线服务模板绑定到 WLAN-Radio 1/0/1 接口

```
[AP] interface WLAN-Radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service-template service1
[AP-WLAN-Radio1/0/1] quit
```

4. 验证配置

配置完成后，在 AP 上执行 **display wlan service-template** 命令，可以看到无线服务模板下安全信息的配置情况如下：

```
[AP] display wlan service-template service1 verbose
Service template name        : service1
Description                  : Not configured
SSID                         : service
SSID-hide                    : Disabled
User-isolation               : Disabled
Service template status      : Enabled
Maximum clients per BSS      : 64
Frame format                 : Dot3
VLAN ID                      : 1
AKM mode                     : Not configured
Security IE                  : Not configured
Cipher suite                 : WEP40
WEP key ID                   : 2
TKIP countermeasure time     : 0
PTK lifetime                 : 43200 sec
GTK rekey                    : Enabled
GTK rekey method             : Time-based
GTK rekey time               : 86400 sec
GTK rekey client-offline     : Enabled
User authentication mode     : Shared-key
Intrusion protection         : Disabled
```

```
Intrusion protection mode    : Temporary-block
Temporary block time         : 180 sec
Temporary service stop time  : 20 sec
Fail VLAN ID                 : Not configured
802.1X handshake             : Disabled
802.1X handshake secure      : Disabled
802.1X domain                : Not configured
MAC-auth domain              : Not configured
Max 802.1X users per BSS     : 4096
Max MAC-auth users per BSS   : 4096
802.1X re-authenticate       : Disabled
Authorization fail mode      : Online
Accounting fail mode         : Online
Authorization                : Permitted
Key derivation               : N/A
PMF status                   : Disabled
Hotspot policy number        : Not configured
Forward policy               : Not configured
Forwarder                    : AC
FT status                    : Disabled
QoS trust                    : Port
QoS priority                 : 0
```

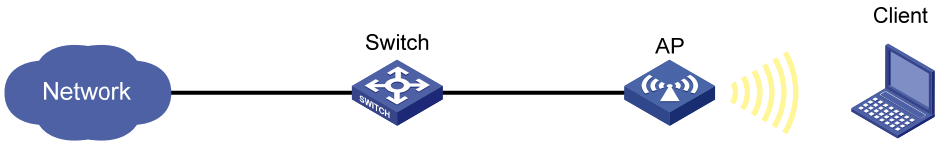
1.11.2 PSK身份认证与密钥管理模式和Bypass认证配置举例

1. 组网需求

- 如 图 1-11 所示，Switch同时作为DHCP server为AP和Client分配IP地址。通过配置客户端PSK密钥 12345678 接入无线网络。
- 客户端链路层认证使用开放式系统认证，用户接入认证使用 Bypass 认证的方式实现客户端可以不需要接入认证直接接入 WLAN 网络的目的。
- 通过配置客户端和 AP 之间的数据报文采用 PSK 身份认证与密钥管理模式来确保用户数据的传输安全。

2. 组网图

图1-11 PSK+Bypass 认证配置组网图



3. 配置步骤

(1) 创建无线服务模板

创建无线服务模板 service1。

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

配置无线服务的 SSID 为 service。

```
[AP-wlan-st-service1] ssid service
```

(2) 配置安全信息

配置 AKM 为 PSK，配置 PSK 密钥，使用明文的字符串 12345678 作为共享密钥。

```
[AP-wlan-st-service1] akm mode psk
[AP-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

配置 CCMP 为加密套件，配置 WPA 为安全信息元素。

```
[AP-wlan-st-service1] cipher-suite ccmp
[AP-wlan-st-service1] security-ie wpa
```

使能无线服务模板。

```
[AP-wlan-st-service1] service-template enable
[AP-wlan-st-service1] quit
```

(3) 将无线服务模板绑定 WLAN-Radio 1/0/1 接口

```
[AP] interface WLAN-Radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service-template service1
[AP-WLAN-Radio1/0/1] quit
```

4. 验证配置

配置完成后，在 AP 上执行 **display wlan service-template** 命令，可以看到无线服务模板的配置情况如下。

```
[AP] display wlan service-template service1 verbose
Service template name        : service1
Description                  : Not configured
SSID                         : service
SSID-hide                    : Disabled
User-isolation               : Disabled
Service template status      : Enabled
Maximum clients per BSS      : 64
Frame format                 : Dot3
VLAN ID                      : 1
AKM mode                     : PSK
Security IE                  : WPA
Cipher suite                 : CCMP
TKIP countermeasure time     : 0
PTK lifetime                 : 43200 sec
GTK rekey                    : Enabled
GTK rekey method             : Time-based
GTK rekey time               : 86400 sec
GTK rekey client-offline     : Enabled
User authentication mode          : Bypass
Intrusion protection         : Disabled
Intrusion protection mode    : Temporary-block
Temporary block time         : 180 sec
Temporary service stop time  : 20 sec
Fail VLAN ID                 : Not configured
802.1X handshake             : Disabled
```

```
802.1X handshake secure      : Disabled
802.1X domain                : Not configured
MAC-auth domain              : Not configured
Max 802.1X users per BSS     : 4096
Max MAC-auth users per BSS   : 4096
802.1X re-authenticate       : Disabled
Authorization fail mode      : Online
Accounting fail mode         : Online
Authorization                : Permitted
Key derivation               : N/A
PMF status                   : Disabled
Hotspot policy number        : Not configured
Forward policy               : Not configured
Forwarder                    : AC
FT status                    : Disabled
QoS trust                    : Port
QoS priority                 : 0
```

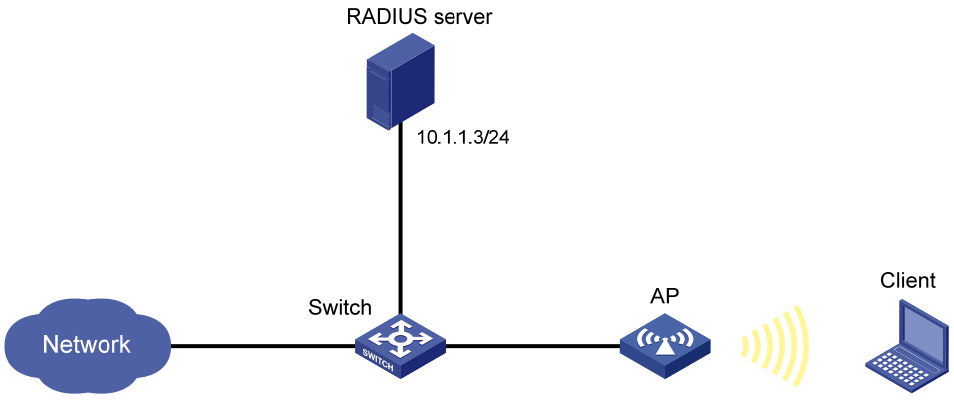
1.11.3 PSK身份认证与密钥管理模式和MAC地址认证配置举例

1. 组网需求

- 如 图 1-12 所示，AP旁挂在Switch上，Switch同时作为DHCP server为AP和Client分配IP地址。通过配置客户端PSK密钥 12345678 接入无线网络。
- 客户端链路层认证使用开放式系统认证，客户端通过 RADIUS 服务器进行 MAC 地址认证的方式，实现客户端可使用固定用户名 abc 和密码 123 接入 WLAN 网络的目的。
- 通过配置客户端和 AP 之间的数据报文采用 PSK 认证密钥管理模式来确保用户数据的传输安全。

2. 组网图

图1-12 PSK 密钥管理模式和 MAC 认证配置组网图



3. 配置步骤

说明

- 下述配置中包含了若干 AAA/RADIUS 协议的配置命令，关于这些命令的详细介绍，请参见“安全命令参考”中的“AAA”。
- 确保 RADIUS 服务器与 AC 路由可达，并成功添加了用户账户，用户名为 abc，密码为 123。

(1) 创建无线服务模板

创建无线服务模板 service1。

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

配置无线服务的 SSID 为 service。

```
[AP-wlan-st-service1] ssid service
```

(2) 配置安全信息

配置 AKM 为 PSK，配置 PSK 密钥，使用明文的字符串 12345678 作为共享密钥。

```
[AP-wlan-st-service1] akm mode psk
[AP-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

配置 CCMP 为加密套件，配置 WPA 为安全信息元素。

```
[AP-wlan-st-service1] cipher-suite ccmp
[AP-wlan-st-service1] security-ie wpa
```

配置用户接入方式为 MAC 地址认证。

```
[AP-wlan-st-service1] client-security authentication-mode mac
```

配置使能无线服务模板。

```
[AP-wlan-st-service1] service-template enable
[AP-wlan-st-service1] quit
```

(3) 创建 RADIUS 方案

创建 RADIUS 方案 radius1 并进入其视图。

```
[AP] radius scheme radius1
```

配置主认证/计费 RADIUS 服务器的 IP 地址为 10.1.1.3，服务器的 UDP 端口号为 1812 和 1813。

```
[AP-radius-radius1] primary authentication 10.1.1.3 1812
[AP-radius-radius1] primary accounting 10.1.1.3 1813
```

配置 AC 与认证/计费 RADIUS 服务器交互报文时的共享密钥为 12345678。

```
[AP-radius-radius1] key authentication simple 12345678
[AP-radius-radius1] key accounting simple 12345678
```

配置发送给 RADIUS 服务器的用户名不携带域名。

```
[AP-radius-radius1] user-name-format without-domain
[AP-radius-radius1] quit
```

说明

发送给服务器的用户名是否携带域名与服务器端是否接受携带域名的用户名、以及服务器端的配置有关:

- 若服务器端不接受携带域名的用户名，或者服务器上配置的用户认证所使用的服务不携带域名后缀，则 Device 上指定不携带用户名（**without-domain**）;
- 若服务器端可接受携带域名的用户名，且服务器上配置的用户认证所使用的服务携带域名后缀，则 Device 上指定携带用户名（**with-domain**）。

(4) 创建认证域并配置使用 RADIUS 方案进行认证、授权、计费

创建认证域（ISP 域）dom1 并进入其视图。

```
[AP] domain dom1
```

配置 MAC 用户使用 RADIUS 方案 radius1 进行认证、授权、计费。

```
[AP-isp-dom1] authentication lan-access radius-scheme radius1
[AP-isp-dom1] authorization lan-access radius-scheme radius1
[AP-isp-dom1] accounting lan-access radius-scheme radius1
[AP-isp-dom1] quit
```

(5) 配置 MAC 地址认证域及用户名和密码

配置认证域为 dom1，用户名为 abc，密码为明文字符串 123。

```
[AP] mac-authentication domain dom1
[AP] mac-authentication user-name-format fixed account abc password simple 123
```

(6) 将无线服务模板绑定到 WLAN-Radio 1/0/1 接口

```
[AP] interface WLAN-Radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service-template service1
[AP-WLAN-Radio1/0/1] quit
```

4. 验证配置

配置完成后，在 AP 上执行 **display wlan service-template** 命令，可以看到无线服务模板的配置情况如下。

```
[AP] display wlan service-template service1 verbose
Service template name          : service1
Description                    : Not configured
SSID                           : service
SSID-hide                      : Disabled
User-isolation                 : Disabled
Service template status        : Enabled
Maximum clients per BSS        : 64
Frame format                   : Dot3
VLAN ID                        : 1
AKM mode                       : PSK
Security IE                    : WPA
Cipher suite                   : CCMP
TKIP countermeasure time       : 0
PTK lifetime                   : 43200 sec
```

```
GTK rekey                     : Enabled
GTK rekey method              : Time-based
GTK rekey time                : 86400 sec
GTK rekey client-offline      : Enabled
User authentication mode      : MAC
Intrusion protection          : Disabled
Intrusion protection mode     : Temporary-block
Temporary block time          : 180 sec
Temporary service stop time   : 20 sec
Fail VLAN ID                  : Not configured
802.1X handshake              : Disabled
802.1X handshake secure       : Disabled
802.1X domain                 : Not configured
MAC-auth domain               : Not configured
Max 802.1X users per BSS      : 4096
Max MAC-auth users per BSS    : 4096
802.1X re-authenticate        : Disabled
Authorization fail mode       : Online
Accounting fail mode          : Online
Authorization                 : Permitted
Key derivation                : N/A
PMF status                    : Disabled
Hotspot policy number         : Not configured
Forward policy                : Not configured
Forwarder                     : AC
FT status                     : Disabled
QoS trust                     : Port
QoS priority                  : 0
```

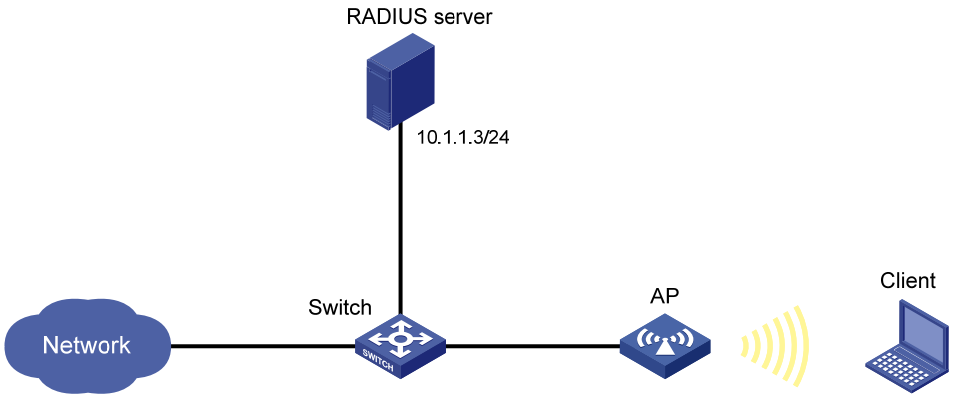
1.11.4 802.1X身份认证与密钥管理模式配置举例

1. 组网需求

- 如 图 1-13 所示，AP旁挂在Switch上，Switch同时作为DHCP server为AP和Client分配IP地址。
- 客户端链路层认证使用开放式系统认证，客户端通过 802.1X 接入认证的方式实现客户端可使用用户名 abcdef 和密码 123456 接入 WLAN 网络的目的。
- 通过配置客户端和 AP 之间的数据报文采用 802.1X 身份认证与密钥管理来确保用户数据的传输安全。

2. 组网图

图1-13 802.1X 认证配置组网图



3. 配置步骤

说明

- 下述配置中包含了若干 AAA/RADIUS 协议的配置命令，关于这些命令的详细介绍，请参见“安全命令参考”中的“AAA”。
- 完成 802.1X 客户端的配置。
- 完成 RADIUS 服务器的配置，添加用户账户,用户名为 abcedf，密码为 123456。

(1) 创建无线服务模板

创建无线服务模板 service1。

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

配置无线服务的 SSID 为 service。

```
[AP-wlan-st-service1] ssid service
```

(2) 配置安全信息

配置 AKM 为 802.1X。

```
[AP-wlan-st-service1] akm mode dot1x
```

配置 CCMP 为加密套件，配置 WPA 为安全信息元素。

```
[AP-wlan-st-service1] cipher-suite ccmp
[AP-wlan-st-service1] security-ie wpa
```

配置用户接入方式为 802.1X 认证。

```
[AP-wlan-st-service1] client-security authentication-mode dot1x
```

配置使能无线服务模板。

```
[AP-wlan-st-service1] service-template enable
[AP-wlan-st-service1] quit
```

(3) 创建 RADIUS 方案

创建 RADIUS 方案 radius1 并进入其视图。

```
[AP] radius scheme radius1
```

配置主认证/计费 RADIUS 服务器的 IP 地址。

```
[AP-radius-radius1] primary authentication 10.1.1.3 1812
[AP-radius-radius1] primary accounting 10.1.1.3 1813
```

配置 AP 与认证/计费 RADIUS 服务器交互报文时的共享密钥为明文字符串 12345。

```
[AP-radius-radius1] key authentication simple 12345
[AP-radius-radius1] key accounting simple 12345
```

配置发送给 RADIUS 服务器的用户名不携带域名。

```
[AP-radius-radius1] user-name-format without-domain
[AP-radius-radius1] quit
```

说明

发送给服务器的用户名是否携带域名与服务器端是否接受携带域名的用户名、以及服务器端的配置有关:

- 若服务器端不接受携带域名的用户名，或者服务器上配置的用户认证所使用的服务不携带域名后缀，则 Device 上指定不携带用户名（**without-domain**）;
- 若服务器端可接受携带域名的用户名，且服务器上配置的用户认证所使用的服务携带域名后缀，则 Device 上指定携带用户名（**with-domain**）。

(4) 创建认证域并配置 RADIUS 方案

创建认证域（ISP 域）dom1 并进入其视图。

```
[AP] domain dom1
```

配置 802.1X 用户使用 RADIUS 方案 radius1 进行认证、授权、计费。

```
[AP-isp-dom1] authentication lan-access radius-scheme radius1
[AP-isp-dom1] authorization lan-access radius-scheme radius1
[AP-isp-dom1] accounting lan-access radius-scheme radius1
[AP-isp-dom1] quit
```

配置使用 dom1 认证域为默认域。

```
[AP] domain default enable dom1
```

(5) 将无线服务模板绑定到 WLAN-Radio 1/0/1 接口

```
[AP] interface WLAN-Radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service-template service1
[AP-WLAN-Radio1/0/1] quit
```

4. 验证配置

配置完成后，在 AP 上执行 **display wlan service-template** 命令，可以看到无线服务模板的配置情况如下。

```
[AP] display wlan service-template service1 verbose
Service template name        : service1
Description                  : Not configured
SSID                         : service
SSID-hide                    : Disabled
User-isolation               : Disabled
Service template status      : Enabled
```

```
Maximum clients per BSS      : 64
Frame format                 : Dot3
VLAN ID                      : 1
AKM mode                     : PSK
Security IE                  : WPA
Cipher suite                 : CCMP
TKIP countermeasure time     : 0
PTK lifetime                 : 43200 sec
GTK rekey                    : Enabled
GTK rekey method             : Time-based
GTK rekey time               : 86400 sec
GTK rekey client-offline     : Enabled
User authentication mode     : 802.1X
Intrusion protection         : Disabled
Intrusion protection mode    : Temporary-block
Temporary block time         : 180 sec
Temporary service stop time  : 20 sec
Fail VLAN ID                 : Not configured
802.1X handshake             : Disabled
802.1X handshake secure      : Disabled
802.1X domain                : Not configured
MAC-auth domain              : Not configured
Max 802.1X users per BSS     : 4096
Max MAC-auth users per BSS   : 4096
802.1X re-authenticate       : Disabled
Authorization fail mode      : Online
Accounting fail mode         : Online
Authorization                : Permitted
Key derivation               : N/A
PMF status                   : Disabled
Hotspot policy number        : Not configured
Forward policy               : Not configured
Forwarder                    : AC
FT status                    : Disabled
QoS trust                    : Port
QoS priority                 : 0
```

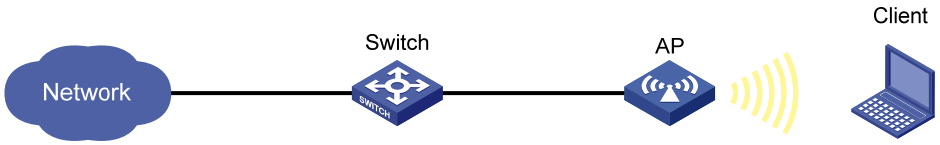
1.11.5 保护管理帧功能配置举例

1. 组网要求

- 如 图 1-14 所示，通过配置客户端PSK密钥 12345678 接入无线网络，Switch做为DHCP服务器为客户端和AP分配IP地址。
- 通过配置客户端和 AP 之间的加密套件为 CCMP、安全 IE 为 RSN 和保护管理帧功能来确保无线网络的安全。

2. 组网图

图1-14 保护管理帧功能配置组网图



3. 配置步骤

(1) 创建无线服务模板

创建无线服务模板 service1。

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

配置无线服务的 SSID 为 service。

```
[AP-wlan-st-service1] ssid service
```

(2) 配置保护管理帧功能

配置保护管理帧功能为 optional。

```
[AP-wlan-st-service1] pmf optional
```

(3) 配置使用 RSNA 安全机制，并使用 PSK 身份认证密钥密钥管理模式、CCMP 加密套件、RSN 安全信息元素

配置 AKM 为 PSK，配置 PSK 密钥为明文的字符串 12345678。

```
[AP-wlan-st-service1] akm mode psk
[AP-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

配置加密套件为 CCMP，配置安全信息元素为 RSN。

```
[AP-wlan-st-service1] cipher-suite ccmp
[AP-wlan-st-service1] security-ie rsn
```

使能无线服务模板。

```
[AP-wlan-st-service1] service-template enable
[AP-wlan-st-service1] quit
```

(4) 将无线服务模板绑定到 WLAN-Radio 1/0/1 接口

```
[AP] interface WLAN-Radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service-template service1
[AP-WLAN-Radio1/0/1] quit
```

4. 验证配置

配置完成后，在 AP 上执行 **display wlan service-template** 命令，可以看到服务模板的配置情况如下。

```
[AP] display wlan service-template service1 verbose
Service template name          : service1
Description                    : Not configured
SSID                           : service
SSID-hide                      : Disabled
User-isolation                 : Disabled
```

```
Service template status      : Enabled
Maximum clients per BSS      : 64
Frame format                 : Dot3
VLAN ID                      : 1
AKM mode                     : PSK
Security IE                  : RSN
Cipher suite                 : CCMP
TKIP countermeasure time     : 0
PTK lifetime                 : 43200 sec
GTK rekey                    : Enabled
GTK rekey method             : Time-based
GTK rekey time               : 86400 sec
GTK rekey client-offline     : Enabled
User authentication mode     : Bypass
Intrusion protection         : Disabled
Intrusion protection mode    : Temporary-block
Temporary block time         : 180 sec
Temporary service stop time  : 20 sec
802.1X handshake             : Disabled
802.1X handshake secure      : Disabled
802.1X domain                : Not configured
MAC-auth domain              : Not configured
Max 802.1X users per BSS     : 4096
Max MAC-auth users per BSS   : 4096
802.1X re-authenticate       : Disabled
Authorization fail mode      : Online
Accoutiong fail mode         : Online
Authorization                : Permitted
Key derivation               : SHA1-AND-SHA256
PMF status                   : Optional
Hotspot policy number        : Not configured
Forward policy               : Not configured
Forwarder                    : AC
FT status                    : Disabled
QoS trust                    : Port
QoS priority                 : 0
```

当有 802.11w 客户端上线，在 AP 上执行 **display wlan client verbose** 命令，可以看到保护管理帧协商结果如下。

```
[AP] display wlan client verbose
Total number of clients: 1

MAC address                      : 5250-0012-0411
Username                         : 11w
Radio ID                         : 1
SSID                             : service
BSSID                            : aabb-ccdd-eeff
VLAN ID                          : 1
Power save mode                  : Active
```

```
Wireless mode                    : 802.11a
QoS mode                         : None
Listen interval                  : 100
RSSI                             : 0
Rx/Tx rate                       : 0/0
Authentication method            : Open system
Security mode                    : RSN
AKM mode                         : PSK
Encryption cipher                : CCMP
User authentication mode         : Bypass
Authorization ACL ID             : N/A
Authorization user profile       : N/A
Roam status                      : Normal
Key derivation                   : SHA256
PMF status                       : Enabled
Online time                      : 0hr 0min 10sec
```

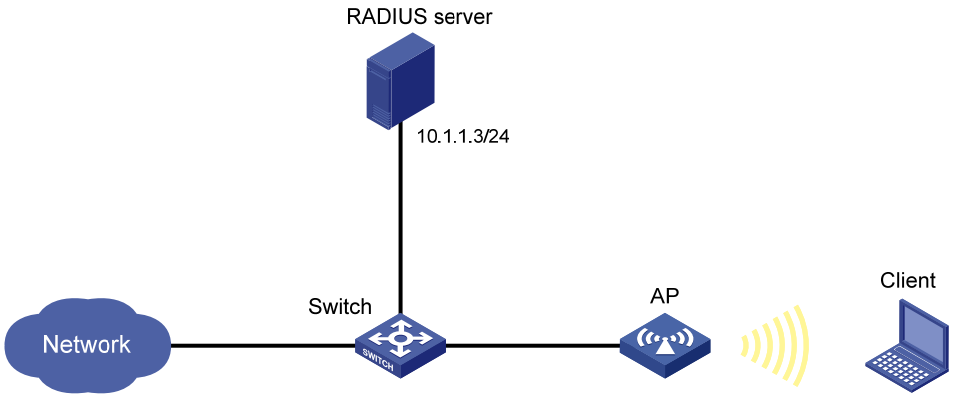
1.11.6 动态WEP配置举例

1. 组网需求

- 如 图 1-15 所示，AP旁挂在Switch上，Switch同时作为DHCP server为AP和Client分配IP地址。
- 客户端链路层认证使用开放式系统认证，客户端通过 802.1X 接入认证的方式实现客户端可使用用户名 abcdef 和密码 123456 接入 WLAN 网络的目的。
- 通过配置客户端和 AP 之间的数据报文采用 802.1X 接入认证与动态 WEP 来确保用户数据的传输安全。

2. 组网图

图1-15 802.1X 认证配置组网图



3. 配置步骤

说明

- 下述配置中包含了若干 AAA/RADIUS 协议的配置命令，关于这些命令的详细介绍，请参见“安全命令参考”中的“AAA”。
- 完成 802.1X 客户端的配置。
- 完成 RADIUS 服务器的配置，添加用户账户,用户名为 abcedf，密码为 123456。

(1) 创建无线服务模板

#创建无线服务模板 service1。

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

配置无线服务的 SSID 为 service。

```
[AP-wlan-st-service1] ssid service
```

(2) 配置动态 WEP 方式加密

#配置 WEP 为 dynamic。

```
[AP-wlan-st-service1] wep mode dynamic
```

配置用户接入方式为 802.1X 认证。

```
[AP-wlan-st-service1] client-security authentication-mode dot1x
```

配置使能无线服务模板。

```
[AP-wlan-st-service1] service-template enable
[AP-wlan-st-service1] quit
```

(3) 创建 RADIUS 方案

创建 RADIUS 方案 radius1 并进入其视图。

```
[AP] radius scheme radius1
```

配置主认证/计费 RADIUS 服务器的 IP 地址。

```
[AP-radius-radius1] primary authentication 10.1.1.3 1812
[AP-radius-radius1] primary accounting 10.1.1.3 1813
```

配置 AP 与认证/计费 RADIUS 服务器交互报文时的共享密钥为明文字符串 123456。

```
[AP-radius-radius1] key authentication simple 123456
[AP-radius-radius1] key accounting simple 123456
```

配置发送给 RADIUS 服务器的用户名不携带域名。

```
[AP-radius-radius1] user-name-format without-domain
[AP-radius-radius1] quit
```

说明

发送给服务器的用户名是否携带域名与服务器端是否接受携带域名的用户名、以及服务器端的配置有关:

- 若服务器端不接受携带域名的用户名，或者服务器上配置的用户认证所使用的服务不携带域名后缀，则 Device 上指定不携带用户名（**without-domain**）;
- 若服务器端可接受携带域名的用户名，且服务器上配置的用户认证所使用的服务携带域名后缀，则 Device 上指定携带用户名（**with-domain**）。

(4) 创建认证域并配置 802.1X 认证方式和 RADIUS 方案

配置 802.1X 认证方式为 EAP。

```
[AP] dot1x authentication-method eap
```

创建认证域（ISP 域）dom1 并进入其视图。

```
[AP] domain dom1
```

配置 802.1X 用户使用 RADIUS 方案 radius1 进行认证、授权、计费。

```
[AP-isp-dom1] authentication lan-access radius-scheme radius1
[AP-isp-dom1] authorization lan-access radius-scheme radius1
[AP-isp-dom1] accounting lan-access radius-scheme radius1
[AP-isp-dom1] quit
```

#配置使用 dom1 认证域为默认域。

```
[AP] domain default enable dom1
```

(5) 将无线服务模板绑定到 Radio 接口

```
[AP] interface WLAN-Radio 1/0/1
[AP-WLAN-Radio1/0/1] service-template service1
[AP-WLAN-Radio1/0/1] quit
```

4. 验证配置

配置完成后，在 AP 上执行 **display wlan service-template** 命令，可以看到无线服务模板的配置情况如下。

```
[AP]display wlan service-template service1 verbose
Service template name          : service1
Description                    : Not configured
SSID                           : service
SSID-hide                      : Disabled
User-isolation                 : Disabled
Service template status        : Enabled
Maximum clients per BSS        : 64
Frame format                   : Dot3
VLAN ID                        : 1
AKM mode                       : Not configured
Security IE                    : Not configured
Cipher suite                   : WEP104
WEP key ID                     : 1
TKIP countermeasure time       : 0
PTK lifetime                   : 43200 sec
```

```
GTK rekey                      : Enabled
GTK rekey method               : Time-based
GTK rekey time                 : 86400 sec
GTK rekey client-offline       : Enabled
User authentication mode       : 802.1X
Intrusionprotection            : Disabled
Intrusionprotection mode       : Temporary-block
Temporary block time           : 180 sec
Temporaryservicestop time      : 20 sec
Fail VLAN ID                   : Not configured
802.1X handshake               : Disabled
802.1X handshake secure        : Disabled
802.1X domain                  : Not configured
MAC-auth domain                : Not configured
Max 802.1X users per BSS       : 4096
Max MAC-auth users per BSS     : 4096
802.1X re-authenticate         : Disabled
Authorization fail mode        : Online
Accounting fail mode           : Online
Authorization                  : Permitted
Key derivation                 : N/A
PMF status                     : Disabled
Hotspot policy number          : Not configured
Forward policy                 : Not configured
Forwarder                      : AC
FT status                      : Disabled
QoS trust                      : Port
QoS priority                   : 0
```

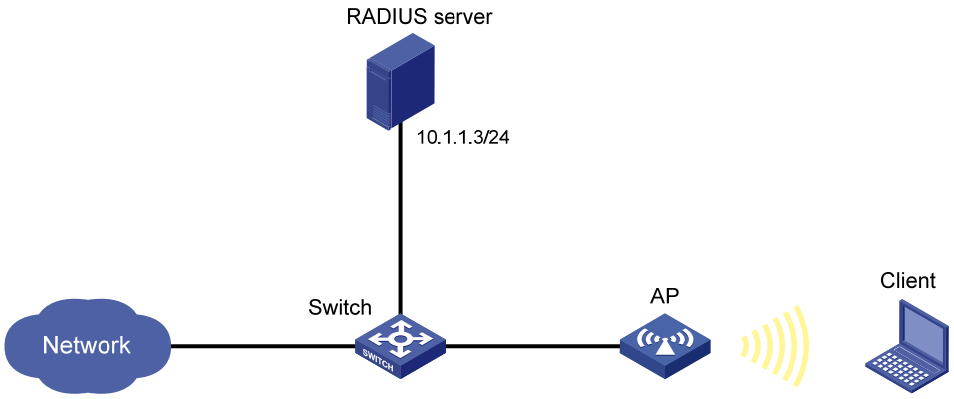
1.11.7 Private-PSK身份认证与密钥管理模式和MAC地址认证配置举例

1. 组网需求

- 如 图 1-16 所示，AP旁挂在Switch上，Switch同时作为DHCP server为AP和Client分配IP地址。配置客户端使用MAC做为PSK密钥接入无线网络。
- 客户端使用 MAC 地址作为用户名和密码接入 WLAN。
- 使用 Private-PSK 身份认证与密钥管理模式来保证用户数据的传输安全。

2. 组网图

图1-16 Private-PSK 密钥管理模式和 MAC 认证配置组网图



3. 配置步骤

说明

- 下述配置中包含了若干 AAA/RADIUS 协议的配置命令，关于这些命令的详细介绍，请参见“安全命令参考”中的“AAA”。
- 确保 RADIUS 服务器与 AC 路由可达，并成功添加了用户账户，用户名为 00-23-12-45-67-7a，密码为 00-23-12-45-67-7a。

(1) 创建无线服务模板

创建无线服务模板 service1。

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

配置无线服务的 SSID 为 service。

```
[AP-wlan-st-service1] ssid service
```

(2) 配置安全信息

配置 AKM 为 Private-PSK。

```
[AP-wlan-st-service1] akm mode private-psk
```

配置 CCMP 为加密套件，配置 WPA 为安全信息元素。

```
[AP-wlan-st-service1] cipher-suite ccmp
[AP-wlan-st-service1] security-ie wpa
```

配置用户接入方式为 MAC 地址认证。

```
[AP-wlan-st-service1] client-security authentication-mode mac
```

使能无线服务模板。

```
[AP-wlan-st-service1] service-template enable
[AP-wlan-st-service1] quit
```

(3) 创建 RADIUS 方案

创建 RADIUS 方案 radius1 并进入其视图。

```
[AP] radius scheme radius1
```

配置主认证/计费 RADIUS 服务器的 IP 地址为 10.1.1.3，服务器的 UDP 端口号为 1812 和 1813。

```
[AP-radius-radius1] primary authentication 10.1.1.3 1812
[AP-radius-radius1] primary accounting 10.1.1.3 1813
```

配置 AC 与认证/计费 RADIUS 服务器交互报文时的共享密钥为 12345678。

```
[AP-radius-radius1] key authentication simple 12345678
[AP-radius-radius1] key accounting simple 12345678
```

配置发送给 RADIUS 服务器的用户名不携带域名。

```
[AP-radius-radius1] user-name-format without-domain
[AP-radius-radius1] quit
```

说明

发送给服务器的用户名是否携带域名与服务器端是否接受携带域名的用户名、以及服务器端的配置有关：

- 若服务器端不接受携带域名的用户名，或者服务器上配置的用户认证所使用的服务不携带域名后缀，则 Device 上指定不携带用户名（**without-domain**）；
- 若服务器端可接受携带域名的用户名，且服务器上配置的用户认证所使用的服务携带域名后缀，则 Device 上指定携带用户名（**with-domain**）。

(4) 创建认证域并配置使用 RADIUS 方案进行认证、授权、计费

创建认证域（ISP 域）dom1 并进入其视图。

```
[AP] domain dom1
```

配置 MAC 用户使用 RADIUS 方案 radius1 进行认证、授权、计费。

```
[AP-isp-dom1] authentication lan-access radius-scheme radius1
[AP-isp-dom1] authorization lan-access radius-scheme radius1
[AP-isp-dom1] accounting lan-access radius-scheme radius1
[AP-isp-dom1] quit
```

(5) 配置 MAC 地址认证域及用户名和密码

配置认证域为 dom1，使用 MAC 地址作为用户名和密码。

```
[AP] mac-authentication domain dom1
[AP] mac-authentication user-name-format mac-address with-hyphen lowercase
```

(6) 将无线服务模板绑定到 WLAN-Radio 1/0/1 接口

```
[AP] interface WLAN-Radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service-template service1
[AP-WLAN-Radio1/0/1] quit
```

4. 验证配置

配置完成后，在 AP 上执行 **display wlan service-template** 命令，可以看到无线服务模板的配置情况如下。

```
[AP] display wlan service-template service1 verbose
Service template name          : service1
Description                    : Not configured
SSID                           : service
SSID-hide                      : Disabled
```

```
User-isolation               : Disabled
Service template status      : Enabled
Maximum clients per BSS      : 64
Frame format                 : Dot3
Seamless roam status         : Disabled
Seamless roam RSSI threshold : 50
Seamless roam RSSI gap       : 20
VLAN ID                      : 1
AKM mode                     : Private-PSK
Security IE                  : WPA
Cipher suite                 : CCMP
TKIP countermeasure time     : 0
PTK lifetime                 : 43200 sec
GTK rekey                    : Enabled
GTK rekey method             : Time-based
GTK rekey time               : 86400 sec
GTK rekey client-offline     : Enabled
User authentication mode     : MAC
Intrusion protection         : Disabled
Intrusion protection mode    : Temporary-block
Temporary block time         : 180 sec
Temporary service stop time  : 20 sec
Fail VLAN ID                 : Not configured
802.1X handshake             : Disabled
802.1X handshake secure      : Disabled
802.1X domain                : Not configured
MAC-auth domain              : Not configured
Max 802.1X users per BSS     : 4096
Max MAC-auth users per BSS   : 4096
802.1X re-authenticate       : Disabled
Authorization fail mode      : Online
Accounting fail mode         : Online
Authorization                : Permitted
Key derivation               : N/A
PMF status                   : Disabled
Hotspot policy number        : Not configured
Forward policy               : Not configured
Forwarder                    : AC
FT status                    : Disabled
QoS trust                    : Port
QoS priority                 : 0
```