

# WLAN 认证和加密技术白皮书

文档版本 02  
发布日期 2012-09-24

华为技术有限公司



**版权所有 © 华为技术有限公司 2012。 保留一切权利。**

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI 和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

## 华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编： 518129

网址： <http://enterprise.huawei.com>

客户服务邮箱： [ChinaEnterprise\\_TAC@huawei.com](mailto:ChinaEnterprise_TAC@huawei.com)

客户服务电话： 4008229999

# 前 言

## 读者对象

本文档针对 WLAN 认证和加密特性，从简介、原理描述和应用三个方面介绍了 WLAN 认证和加密特性。






本文档与其它类型手册相结合，便于读者深入掌握特性的实现原理。

本文档主要适用于以下工程师：

- 网络规划工程师
- 调测工程师
- 数据配置工程师
- 系统维护工程师

## 符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
 危险	表示有高度或中度潜在危险，如果不能避免，可能会导致人员死亡或严重伤害。
 警告	表示有低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
 注意	表示有潜在风险，如果不能避免，可能会导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 窍门	能帮助您解决某个问题或节省您的时间。
 说明	正文的附加信息，是对正文的强调和补充。

## 修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

### 文档版本 02 (2012-09-24)

相对于版本 01 (2010-04-29)的变化如下：

修改：

- [WPA-PSK 认证](#)
- [802.1X](#)
- [MAC 认证](#)

### 文档版本 01 (2010-04-29)

第一次正式发布。

目 录

前 言..... ii

1 WLAN 认证和加密技术白皮书..... 1

    1.1 介绍 ..... 1

    1.2 原理描述 ..... 2

        1.2.1 概述 ..... 2

        1.2.2 STA 身份验证..... 6

        1.2.3 用户身份验证与加密..... 9

        1.2.4 数据加密技术.....24

    1.3 应用 .....36

        1.3.1 WPA+802.1X 认证示例 .....36

        1.3.2 Portal 认证 .....38

# 1 WLAN 认证和加密技术白皮书

## 关于本章

- 1.1 介绍
- 1.2 原理描述
- 1.3 应用

## 1.1 介绍

### 定义

当前以 802.11 为标准的 WLAN 为广大用户提供了越来越高的无线接入带宽，越来越多的用户开始试用 WLAN 网络，同时对 WLAN 的安全性也提出了越来越高的要求。如何保护用户敏感数据的安全，保护用户的隐私，是众多 WLAN 用户非常关心的问题。

由于 WLAN 无线侧数据是在空中自由传播的，这些数据可以被任何合适的接收装置获取的，所以 WLAN 由最初发展到现在，其无线侧数据的安全性一直备受关注，相关的认证、加密技术也不断演进，不断加强。至今，WLAN 系统已具备了一系列的安全机制，以满足各种应用场景的实际需求，小到家庭无线网络，大到企业网 WLAN、校园网 WLAN，乃至运营商统一建立的广域覆盖的 WLAN，都有相应合适的认证、加密技术来保护用户无线数据的安全。

具体来说，WLAN 接入安全主要包括安全各类属性的配置、无线侧帧的加密和解密，密钥管理等功能。

WLAN 安全共分为三个方面：

- STA 身份验证：对客户端的认证，只有通过认证后，才能进入后续的关联阶段。
- 数据加密：对数据报文进行加密，保证只有特定的设备才可以对接收到报文成功解密。无线网络中的其他设备虽然可以接收到数据报文，但是由于没有对应的密钥，无法对数据报文解密，从而实现 WLAN 数据的安全性保护。

- 用户身份验证与加密：对用户进行区分，并在用户访问网络之前限制其访问权限。使用户在进行链路认证时只允许有限的网络访问权限，只有确定用户身份后才会允许完整的网络访问。

## 目的

WLAN 接入安全特性主要解决无线侧安全问题，避免无线局域网中的传播数据在传输的过程中被非法捕获。主要包含两个方面：

- 防止未授权用户访问网络资源。
- 保护数据完整性和数据传输私密性。

## 受益

用户受益

用户的隐私和敏感数据的安全得到保护。

## 1.2 原理描述

### 1.2.1 概述

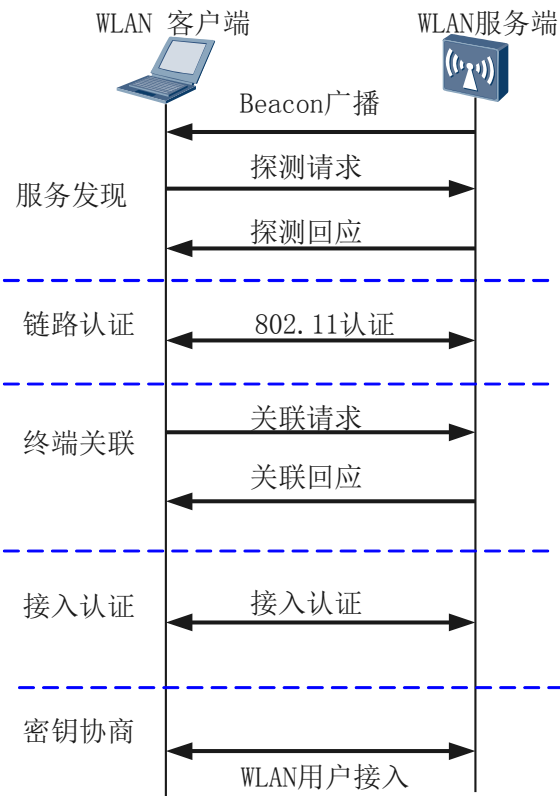
WLAN 网络的目的是为无线用户提供网络接入服务，实现用户访问网络资源（例如 Internet）的需求。

如果网络服务没有使用任何接入认证，客户端可以直接成功的接入到网络服务中；如果网络服务指定了接入认证方式，则 WLAN 服务端会触发对用户的接入认证，只有接入认证成功后，WLAN 客户端才可以成功的访问网络。

可以简单将 WLAN 组网分成 WLAN 客户端和 WLAN 服务端两部分，WLAN 客户端为有无线网卡的主机设备，而 WLAN 服务端则为 AP 设备。

下图简单描述了客户端接入到 WLAN 服务的协商过程。

图1-1 WLAN 用户接入



1. WLAN 服务发现

使用任何网络之前，首先必须找出网络何在。使用有线网络，要找出网络所在并不难，只要循着网线或者找到墙上的插座即可。在无线领域中，STA 加入任何无线网络之前，必须先经过一番辨识的工作。这种于所在区域辨识现有网络的程序称为 WLAN 服务发现过程。

- WLAN 服务端会主动发送 Beacon 通告提供的 WLAN 服务，客户端可以根据该报文确定周围存在的 WLAN 服务；
- WLAN 客户端可以指定 SSID（WLAN 服务的标识）或者使用广播 SSID（即没有指定 SSID）主动地探测是否存在指定的网络，WLAN 服务端存在指定的 WLAN 服务，会发送确认信息给客户端。

服务发现成功后进入链路认证过程。

2. 链路认证

只要工作站打算连接到网络，就必须进行 802.11 “身份认证”。

当前 802.11 的链路认证支持两种认证方式：开放认证（Open System Authentication）和 Shared-Key 认证（Shared Key Authentication）。两种认证方式都是在 IEEE802.11 中定义，802.11 链路认证通过 Authentication 报文实现。

3. 终端关联

一旦完成身份认证，STA 就可以跟基站进行连接（或者跟新的基站进行重新连接），以便获得网络的完全访问权。



在 WLAN 服务发现过程中，WLAN 客户端已经获得了当前服务的配置和参数（WLAN 服务端会在 Beacon 和 Probe Response 报文中携带，例如接入认证算法以及加密密钥）。WLAN 客户端在发起的 Association 或者 Re-association 请求时，会携带 WLAN 客户端自身的各种参数，以及根据服务配置选择的各种参数（主要包括支持的速率，支持的信道，支持的 QoS 的能力，以及选择的接入认证和加密算法）。

WLAN 客户端和 WLAN 服务端成功完成链路服务协商，表明两个设备成功建立了 802.11 链路。对于没有使能接入认证的服务，客户端已经可以访问 WLAN 网络；如果 WLAN 服务使能了接入认证，则 WLAN 服务端会发起对客户端的接入认证。

#### 4. 接入认证

用户接入认证实现了对接入用户的身份认证，为网络服务提供了安全保护。接入认证主要有 802.1X 认证、PSK 认证、Portal 认证、MAC 认证等方式。其中 802.1x 接入认证、MAC 接入认证、Portal 认证可以支持对有线用户和 WLAN 无线接入用户进行身份认证，而 PSK 认证则是专门为 WLAN 无线用户提供认证的一种方法。

WLAN 服务应用中，对于 WPA（Wi-Fi Protected Access）用户或者 WPA2 用户需要进行 EAPOL-Key 密钥协商。根据 WLAN 协议服务定义，对于 WPA 服务，需要和 802.1x 接入认证以及 PSK 接入认证配合使用；在 802.11 链路协商的过程中，可以确定用户使用的接入认证算法；并且在链路协商成功后触发对用户的接入认证；随后需要为该接入用户的协商密钥；之后 WLAN 客户端才可以访问 WLAN 网络。

#### 5. 密钥协商

密钥协商为数据安全提供有力保障，为了保证 WLAN 数据的安全，IEEE802.11i 和 IEEE 802.1X 定义了 EAPOL-Key 密钥协商机制（也称 4-Way Handshake），WLAN 就是用该机制实现 WLAN 服务端和 WLAN 客户端的密钥协商，协商出来的密钥将作为 802.11 数据传输过程中的加密/解密密钥。

对于支持 WPA 和 RSN（robust security network）服务的 WLAN，需要进行 EAPOL-Key 密钥协商。密钥协商过程在逻辑上可以看作接入认证的一部分，所以只有在 EAPOL-Key 密钥协商成功以后，接入认证才会打开端口，允许用户的报文通过。

WLAN 密钥协商主要包括四次握手密钥协商和组密钥协商过程，这两种密钥协商都通过 EAPOL-Key 报文协商实现。WLAN 客户端和 WLAN 服务端使用四次握手机制协商该客户端的单播数据报文使用的密钥，而 WLAN 服务端可以通过组密钥协商过程将广播和组播使用的密钥通知所有的 WLAN 客户端。

#### 6. 数据加密

使用者身份确定无误并赋予访问权限后，网络必须保护用户所传送的数据不被窥视。保护无线链路数据的私密性，是所有无线网络需要面对的挑战。数据的私密性通常是靠加密协议来达成，只允许拥有密钥并经过授权的用户访问数据，确保数据在传输过程中未遭篡改。

华为 WLAN 认证加密特性详细内容如表 1-1

表1-1 华为 WLAN 认证加密特性

类别	特性
WEP	<ul style="list-style-type: none"> <li>WEP 是 1999 年 9 月通过的 IEEE802.11 标准的一部分，使用 RC4(Rivest Cipher)串流加密技术达到机密性。</li> <li>支持开放式系统（open system authentication）和共享密钥（shared key authentication）两种认证方式。</li> <li>WEP 是接入点和客户端之间以“RC4”方式对分组信息进行加密的技术，密钥一旦设置，就无法自动更新，密码容易被破解，目前使用比较少。</li> <li>开放式系统是运营商网络的主流认证方式，一般结合 Portal 认证使用。</li> </ul>
WPA/WPA2-PSK	<ul style="list-style-type: none"> <li>WPA 是 Wi-Fi 保护接入（Wi-Fi Protected Access）的缩写，是由 Wi-Fi 联盟所推行的商业标准，实现了 IEEE802.11i 标准的大部分，是在 802.11i 完备之前替代 WEP 的过渡方案，采用 TKIP（临时密钥完整性协议）加密算法加密。</li> <li>WPA2 是基于最终的 802.11i 标准，是完备的 802.11i 标准，是 WPA 的第二版，使用 CCMP（计数器模式及密码块链消息认证码协议）加密算法进行数据加密。</li> <li>WPA/WPA2-PSK，要求在每个 WLAN 节点(AP、无线路由器、网卡等)预先输入一个密钥。只要密钥吻合，客户就可以获得 WLAN 的访问权。由于这个密钥仅仅用于认证过程，而不适用于加密过程，因此不会导致诸如使用 WEP 密钥来进行 802.11 预共享认证那样严重的安全问题。</li> <li>不需要安装客户端。</li> <li>使用较少，因为没有人来维护 WPA/WPA2 需要的密码。</li> </ul>
802.1X	<ul style="list-style-type: none"> <li>802.1X 只定义了身份验证框架，并非一套完整的规范。具体的认证需要其他协议，支持的认证方式有 EAP、LEAP、EAP-TLS、EAP-TTLS、PEAP 等。</li> <li>802.1x 协议为二层协议，不需要到达三层，客户端和服务端之间的双向认证，能够很好的支持组播。</li> <li>通常需要安装特定客户端软件，如果用户只做准入不做策略控制，则目前常用的 iso, android, windows 操作系统都支持 802.1X，不需要安装客户端。</li> <li>企业网大量使用，运营商网络使用少。</li> </ul>
WAPI	<ul style="list-style-type: none"> <li>WAPI 是我国提出的无线局域网标准（GB15629.11），标准中包含了全新的 WAPI（WLAN Authentication and Privacy Infrastructure）安全机制，这种安全机制由 WAI（WLAN Authentication Infrastructure）和 WPI（WLAN Privacy Infrastructure）两部分组成。</li> <li>WAPI 提供两种鉴别和密钥管理方法：基于证书的方式和基于预共享密钥的方式。</li> <li>WAPI 相对 WPA 由二元认证改成三元认证；加密算法的改变，由 CCMP 改成 SMS4。</li> </ul>

类别	特性
	<ul style="list-style-type: none"><li>WAPI 由于是国家标准，国内市场一般都要求支持，海外市场使用较少。</li></ul>
Portal	<ul style="list-style-type: none"><li>Portal 认证也称 Web 认证，或 DHCP+WEB 认证，使用标准 Web 浏览器（例如 IE）即可，不需要安装特殊的客户端软件。</li><li>认证前用户终端已经获得 IP 地址，用户与接入服务器中间可以存在路由器等三层设备，接入服务器的报文中可能没有用户 MAC 地址信息，无法做到 MAC、IP 的绑定。</li><li>运营商和企业网中大量使用。</li></ul>
Mac	<ul style="list-style-type: none"><li>MAC 认证是另外一种接入认证方式。MAC 接入认证主要为客户端以自己的 MAC 地址作为身份凭据到设备端进行认证。</li><li>登录时不需要输入用户名和密码，在安全要求不高的场合使用较为广泛。</li></ul>

华为 WLAN 认证加密特性可以结合不同场景为客户量身提供多种认证组合解决方案，例如运营 WLAN 网络。在运营商 WLAN 网络中，通常使用 Open System+Portal 认证方式，用户连接运营商 WLAN 网络，Portal 服务器强制推动认证服务界面，用户通过认证后可以访问网络。认证服务界面通常伴有广告，推送 MAC 绑定功能，用户选择 MAC 绑定功能，则下一次再连接运营商的 WLAN 网络，直接使用 MAC 认证不需要再输入用户名和密码就可以访问网络。

1.2.2 STA 身份验证

802.11 标准要求 STA 在打算连接到网络时，必需进行 802.11 “链路认证”。由于这种认证并没有传递或验证任何加密密钥，也没有进行相互认证过程，所以可以将这个链路认证视为 STA 连接到 WLAN 网络时的握手过程的起点。

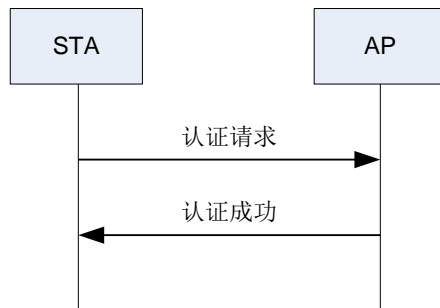
STA 身份认证主要有两种方式：开放式和共享密钥式。有些产品也可以提供 MAC 地址过滤功能，可以在身份验证阶段过滤掉未授权的 STA 的 MAC 地址。

开放系统认证（Open system authentication）

开放系统认证是 802.11 要求必备的一种方法。在这种方式下，接入点并未验证 STA 的真实身份，STA 以 MAC 地址作为身份证明，这种验证方式可以让所有符合 802.11 标准的终端都可以接入到 WLAN 网络中来。开放系统身份验证比较适合有众多用户的运营商部署的大规模的 WLAN 网络。

开放系统认证只有两个步骤，只确认 AP 和网卡采用了相同的鉴权方式，不对 WEP 加密密钥进行验证。认证过程如图 1-2 所示。

图1-2 开放系统认证过程



开放系统认证的过程为：

1. STA 发送一个认证请求给选定的 AP。
2. 该 AP 发送一个认证成功响应报文给客户端确认该认证并在 AP 上注册客户端。

开放系统验证的优缺点：

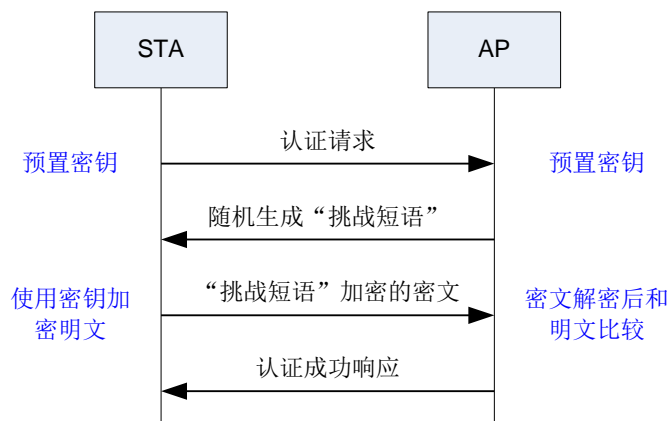
- 优点：开放认证是一个基本的验证机制，可以使用不支持复杂的认证算法的无线设备。802.11 协议中认证是面向连接的，对于需要允许设备快速进入网络的场景，可以使用开放式身份验证。
- 缺点：开放认证没办法检验客户端是否是一个有效的客户端，而不是黑客客户端。如果使用不带 WEP 加密的开放验证，任何知道无线局域网 SSID 的用户都可以访问网络。

## 共享密钥认证（Shared-key authentication）

共享密钥认证是除开放系统认证以外的另外一种链路认证机制。

共享密钥认证必须使用 WEP 加密方式，要求 STA 和 AP 使用相同的共享密钥（key），通常被称为静态 WEP 密钥。认证过程包含 4 步，后三步包含了一个完整的 WEP 加密/解密过程（框架与 CHAP 类似），对 WEP 加密的密钥进行了验证，确保了网卡在发起关联时与 AP 配置了相同的加密密钥。共享密钥的认证过程如图 1-3 所示。

图1-3 共享密钥认证过程



共享密钥认证的过程为：

1. STA 先向 AP 发送认证请求。
2. AP 会随机产生一个“挑战短语”发送给 STA。
3. STA 会将接收到的“挑战短语”拷贝到新的消息中，用密钥加密后再发送给 AP。
4. AP 接收到该消息后，用密钥将该消息解密，然后对解密后的字符串和最初给 STA 的字符串进行比较。
  - 如果相同，则说明 STA 拥有与 AP 相同的共享密钥，即通过了共享密钥认证。
  - 如果不同，则共享密钥认证失败。

共享密钥认证的优缺点：

- 优点：由于采用了 WEP 加密方式对密钥进行保护，空口密钥数据不再明文传输，提供比开放认证更安全的认证机制。
- 缺点：
  1. 可扩展性不佳，因为必须在每台设备上配置一个很长的密钥字符串；
  2. 不是很安全，静态密钥的使用时间非常长，直到手工重新配置了新密钥为止。密钥的使用时间越长，恶意用户便有更长的时间来收集从它派生出来的数据，并最终通过逆向工程破解密钥。静态 WEP 密钥是比较容易被破解的。

早期 WLAN 常用的加密方式是 WEP，这个在下面的章节中将详细介绍。不需要认证的系统称为开放式系统，需要认证的系统称为共享密钥系统。但不管是哪种系统，都可以选择是否加密。WEP 认证加密支持下列组合方式：

- 开放+明文，具体配置如下：

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wep
[Quidway-wlan-sec-prof-huawei] wep authentication-method open-system
```

- 开放+密文，具体配置如下：

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wep
[Quidway-wlan-sec-prof-huawei] wep authentication-method open-system data-encrypt
```

- 共享密钥+明文，具体配置如下：

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wep
[Quidway-wlan-sec-prof-huawei] wep key wep-40 pass-phrase 0 simple 12345
[Quidway-wlan-sec-prof-huawei] wep default-key 0
```

- 共享密钥+密文，具体配置如下：

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
```

```
[Quidway-wlan-sec-prof-huawei] security-policy wep
[Quidway-wlan-sec-prof-huawei] wep key wep-40 pass-phrase 0 simple 12345
[Quidway-wlan-sec-prof-huawei] wep default-key 0
```

配置和管理静态密码非常复杂，因此一些产品支持动态 WEP，即在开放系统下，采用 802.1X 认证来协商密钥。但由于 WEP 本身安全性差，且动态 WEP 和 WPA 流程过程类似，反而不如直接使用 WPA，因此动态 WEP 现在已基本不再使用。动态 WEP 的组合方式为：开放+802.1X+密文。

## MAC 地址过滤

网络上各个 AP 均有一份允许访问 WLAN 网络的 MAC 地址列表（白名单），也可以有一份禁止访问 WLAN 网络的 MAC 地址列表（黑名单）。根据事先配置的策略，可以只允许白名单的 MAC 接入，或者只禁止黑名单中的 MAC 地址接入。

MAC 地址过滤与其说是一种认证方式，更应该是一种访问控制方式。由于 MAC 地址很容易被伪造或复制，这种 STA 身份验证方法不建议单独使用，除非一些旧设备无法提供更好的机制。

STA 黑名单的配置如下：

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] sta-access-mode ap 0 blacklist
[Quidway-wlan-view] sta-blacklist 286E-D488-B74F
```

STA 白名单的配置如下：

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] sta-access-mode ap 0 whitelist
[Quidway-wlan-view] sta-whitelist 286E-D488-B74F
```

## 1.2.3 用户身份验证与加密

相对于简单的 STA 身份验证机制，用户身份验证可谓是一大进步，体现在：

- 在进行链路认证时只允许有限的网络访问，只有确定用户身份后才会允许完整的网络访问。
- 可以对用户进行区分并在用户访问网络之前限制访问权限。
- 对于网络协议而言，链路层认证可以配合任何网络层协议使用。

用户身份验证主要包含以下几大方面：

- WPA/WPA2-PSK 认证
- 802.1X 认证
- WAPI 认证
- Portal 认证
- MAC 认证

## WPA-PSK 认证

WPA-PSK 是一种通过 Pre-shared key 进行认证，并以 Pre-shared key 作为 PMK 协商临时密钥的认证加密方式。

WPA-PSK 要求在 STA 侧预先配置 Key，通过与 AP 或 AC 侧的 4 次握手协商协议来验证 STA 侧 Key 的合法性。

WPA-PSK 加密在 STA 与 AP 间的认证和关联过程中采用与 Open 的 WEP 方式一致，STA 与 AP 关联成功后，进入四次握手协商密钥过程。

四次握手过程主要是为了产生 PTK (Pairwise Transient Key) 和 GTK (Group Temporal Key)，PTK 用来加密单播无线报文，GTK 用来加密组播和广播无线报文。

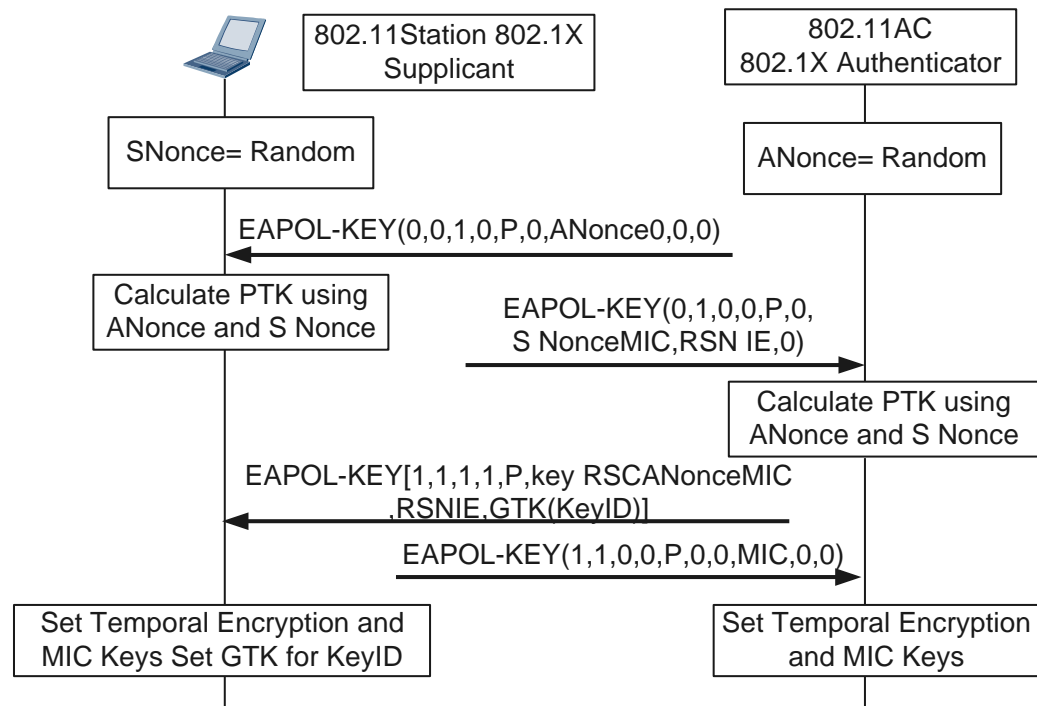
在 802.11i 里定义了两种密钥层次模型，一种是成对密钥层次结构，主要用来描述一对设备之间的所有密钥；一种是组密钥层次结构，主要用来描述全部设备所共享的各种密钥。

在成对密钥层次结构下，TKIP 加密方式根据主密钥衍生出四个临时密钥，每个临时密钥 128 比特，这四个 key 分别是 EAPOL-Key-Encryption-Key、EAPOL-Key-Integrity-Key、Data-Encryption-Key 和 Data-Integrity-Key，前面两个 EAPOL MIC 密钥和 EAPOL 加密密钥用于在初始化握手信息过程中保护 WLAN 客户端和 WLAN 服务端的通信。后两个用在 WLAN 客户端和 WLAN 服务端的加密数据和保护数据不被更改。对于 CCMP 加密的方式下，衍生出的临时密钥只有三个，因为数据的完整性和加密密钥是同一个。

在组密钥层次结构下，TKIP 的加密方式下根据 GMK (128 比特) 衍生出 2 个密钥，用来 WLAN 客户端和 WLAN 服务端之间的多播数据加密和完整性加密。而 CCMP 的方式数据加密密钥和数据 MIC 密钥合成一个密钥用来多播数据加密和完整性加密。

- 四次单播密钥协商过程

图1-4 EAPOL-Key 单播密钥协商



如图 1-4 所示，EAPOL-Key 单播密钥协商流程说明如下：

1. WLAN 服务端发送 EAPOL-Key 帧给 WLAN 客户端，帧中包含随机数 ANonce(nonce 是为了防范重放攻击的随机值，包括 ANonce 和 SNonce 两种，区别在于 ANonce 是 AC 随机产生并发送给 STA，SNonce 是 STA 收到 ANonce 后随机产生的)。
  2. WLAN 客户端根据 PMK、ANonce、SNonce、自己的 MAC 地址、WLAN 服务端的 MAC 地址计算出 PTK，WLAN 客户端发送 EAPOL-Key 帧给 WLAN 服务端，帧中包含 Snonce、RSN 信息元素、EAPOL-Key 帧的消息完整码(MIC)。
  3. WLAN 服务端根据 PMK、ANonce、SNonce、自己的 MAC 地址、WLAN 客户端的 MAC 地址计算出 PTK，并校验 MIC，核实 WLAN 客户端的 PMK 是否和自己的一致。
  4. WLAN 服务端发送 EAPOL-Key 帧给 WLAN 客户端，并通知 WLAN 客户端安装密钥，帧中包含 Anonce、RSN 信息元素、帧 MIC、加密过的 GTK。
  5. WLAN 客户端发送 EAPOL-Key 帧给 WLAN 服务端，并通知 WLAN 服务端已经安装并准备开始使用加密密钥。WLAN 服务端收到后本端安装加密密钥。
- 二次组播密钥协商过程

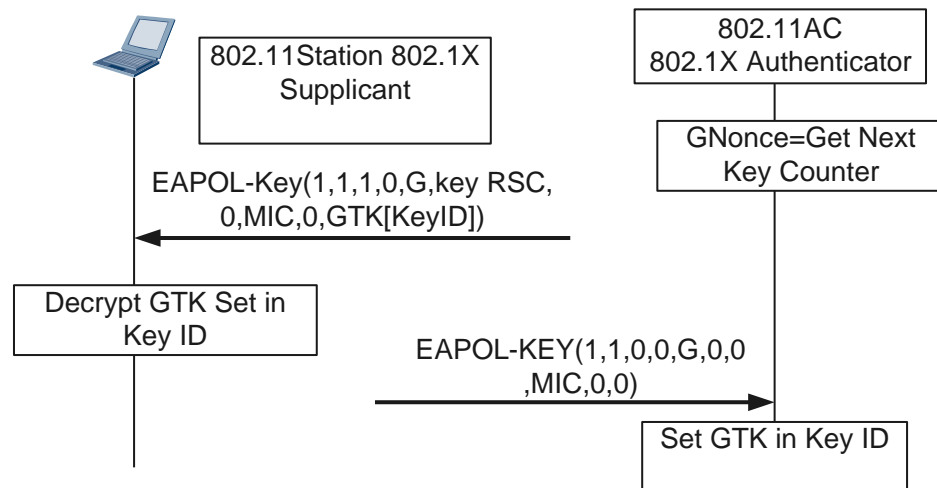
两次握手主要是用来产生组播密钥，主要有两个消息，第一个发送密钥，第二个确认密钥已经安装。

当一个新用户上线后，经过四次握手产生 PTK 并安装密钥开始加密后，开始进行两次握手，由 WLAN 服务端计算出 GTK，并用该用户的单播密钥加密发送给 WLAN 客户端，WLAN 客户端根据之前四次握手的临时密钥解密。



新用户上线，并不一定会产生两次握手，GTK 可以有四次握手中的第三个消息产生，如果不产生的话，可以由两次握手产生，两次握手也可以用来组密钥的更新。

图1-5 EAPOL-Key 多播密钥协商



如图 1-5 所示，EAPOL-Key 多播密钥协商流程说明如下：

1. WLAN 服务端计算出 GTK，用单播密钥加密 GTK，发送 EAPOL-Key 帧给 WLAN 客户端。
2. WLAN 客户端收到 EAPOL-Key 帧后，验证 MIC，解密 GTK，安装组播加密密钥 GTK，并发送 EAPOL-Key 确认消息给 WLAN 服务端。
3. WLAN 服务端收到 EAPOL-Key 确认帧后，验证 MIC，安装 GTK。

## 802.1X

802.1X 协议起源于无线局域网（WLAN）的发展和应用，WLAN 具有移动性、开放性的特点，因此需要对用户的端口接入进行认证控制，以保护无线频谱资源的利用和网络安全。802.1X 协议应用于有线局域网中，通过对用户接入端口的认证控制，达到对用户管理的目的。

802.1X 是基于端口的网络接入控制协议，提供了一个认证过程框架，支持多种认证协议。在 802.1X 中，不同的认证协议统一使用 EAP 封装格式。也就是说，802.1X 只是对认证进行控制，是接入认证的手段，具体认证还需要其它认证协议。

802.1X 在局域网接入控制设备的端口一级对所接入的设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源，相当于物理连接被断开。

802.1x 认证以安全可靠，易于实现，应该用灵活，行业标准等特点在 3G 和 WLAN 融合的运营商网络和企业网络中都大量应用。

- 安全可靠：在无线局域网网络环境中 802.1X 需要结合 EAP-TLS，EAP-PEAP 等实现对证书密钥的动态分配，克服无线局域网接入中的安全漏洞。下文中会具体介绍。

- 容易实现，应用灵活：802.1x 认证保留了传统 AAA 认证的网络架构，可以利用现有的 RADIUS 设备，易于实现且可以灵活控制认证的颗粒度，用于对单个用户连接、用户组或者是对接入设备进行认证，认证的层次可以进行灵活的组合。
- 行业标准：IEEE 标准，和以太网标准同源，可以实现和以太网技术的无缝融合，在客户端方面 Windows，Linux，ISO，androids 都支持该协议。

### 基于 EAP-TLS 的 802.1X 认证

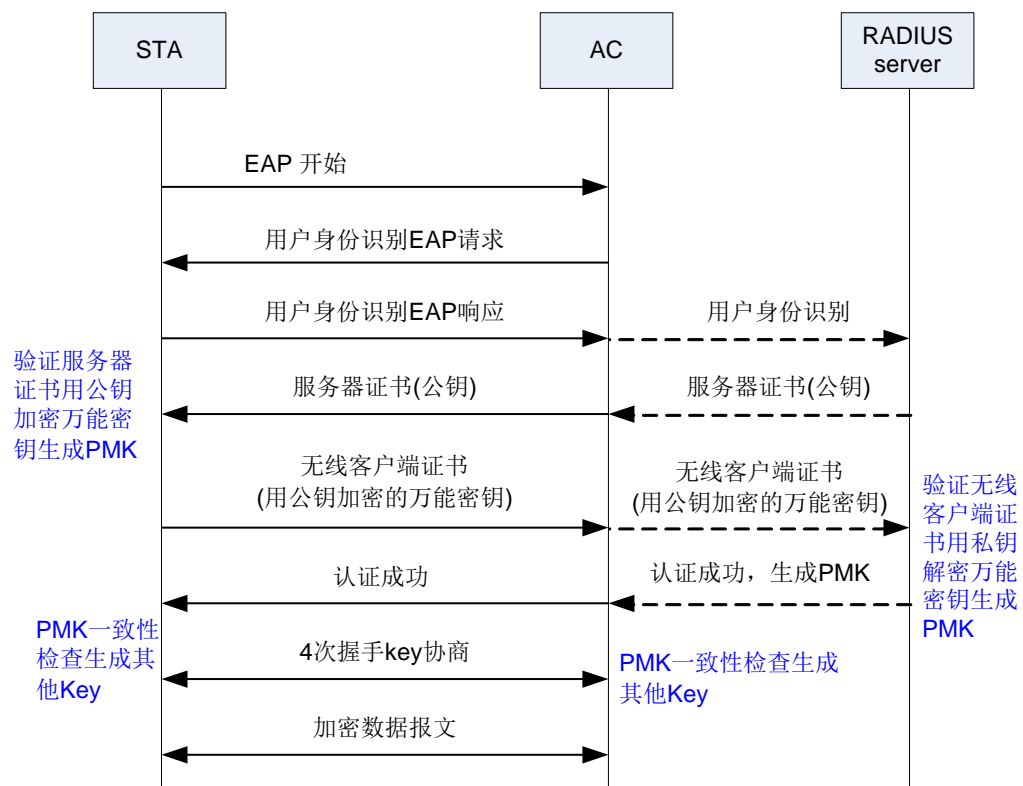
可扩展认证协议-传送层安全 EAP-TLS(Extensible Authentication Protocol-Transport Layer Security)使用传送层安全协议 TLS(Transport Layer Security)，TLS 是一种替代安全套接层 SSL(Secure Socket Layer)协议的 IETF 标准协议，TLS 可以提供公共域上的安全通信和数据传送服务，并能防范窃听和报文篡改等攻击行为。EAP-TLS 使用 PKI，因而必须满足以下三方面需求：

- STA 必须获得证书，网络才能对其进行认证。
- AAA 服务器需要一个证书，STA 才能确认服务器的真实性。
- 证书认证机构 CA(Certification Authority)服务器必须为 AAA 服务器和 STA 发放证书。

EAP-TLS 认证进程，无线 STA 使用开放系统认证与 AP 建立关联。在 Radius 服务器认证通过之前，AP 会限制（或拒绝）除 EAP 流量之外的所有流量。

基于 EAP-TLS 的 802.1X 认证接入过程如图 1-6 所示。

图1-6 基于 EAP-TLS 的 802.1X 认证流程图



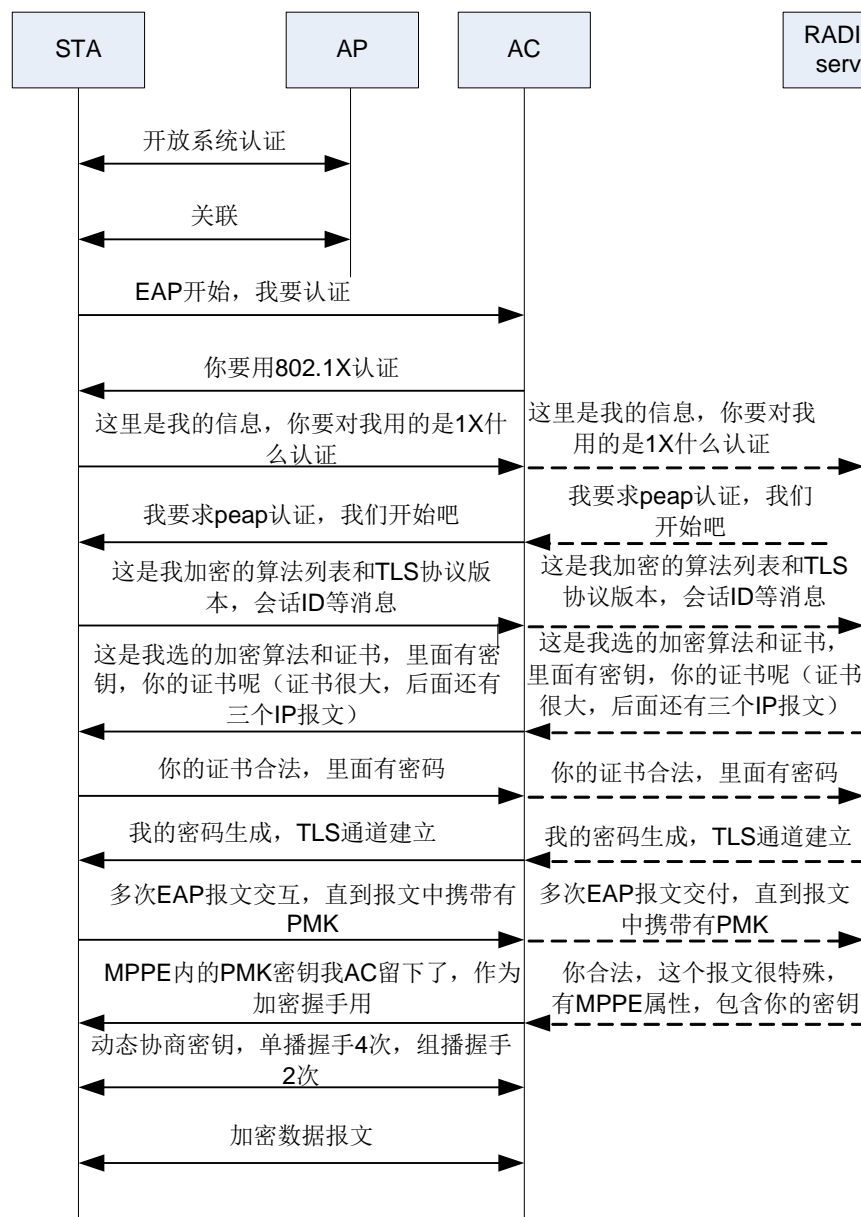
### 基于 EAP-PEAP 的 802.1X 认证

802.1X 在 WLAN 上使用时，一般不用 MD5 的 EAP，而是使用保护模式的 EAP，如 EAP-PEAP，EAP-TLS，EAP-SIM 等。最常用就是 EAP-PEAP。EAP-PEAP（受保护的可扩展验证协议）是由 Microsoft、Cisco、RAS Security 联合开发安全认证协议，Windows 操作系统默认支持。

在大型企业网络中，通常采用这种方式。同 EAP-TLS 相比，在 TLS 协商阶段是完全一样的，都是完成双向认证或仅对服务器端的认证，建立 TLS 安全隧道。第二阶段是在安全隧道的保护下完成用户认证，目前，PEAP 仅支持使用 EAP 进行认证，而 EAP-TTLS 除了 EAP 外，还支持 PAP、CHAP 等用户认证方式。

基于 EAP-PEAP 的 802.1X 认证接入过程如图 1-7 所示。

图1-7 基于 EAP-PEAP 的 802.1X 认证流程图



## WAPI 认证

WAPI 是 WLAN Authentication and Privacy Infrastructure（无线局域网鉴别与保密基础结构）的简称，是中国提出的、以 802.11 无线协议为基础的无线安全标准，WAPI 的以太类型字段为 0x88B4。WAPI 协议由以下两部分构成：

- **WAI**：是 WLAN Authentication Infrastructure（无线局域网鉴别基础结构）的简称，是用于无线局域网中身份鉴别和密钥管理的安全方案；
- **WPI**：是 WLAN Privacy Infrastructure（无线局域网保密基础结构）的简称，是用于无线局域网中数据传输保护的安全方案，包括数据加密、数据鉴别和重放保护等功能。

WAPI 是一种仅允许建立 RSNA（Robust Security Network Association）的安全服务，提供比 WEP 和 WPA 更强的安全性。WAPI 可通过信标帧的 WAPI IE（Information Element）中的指示来标识。

WAPI 是基于三元对等鉴别的访问控制方法在无线局域网领域应用的一个实例，它由两部分组成：**WAI**（WLAN authentication infrastructure）和 **WPI**（WLAN privacy infrastructure）。

如果 WLAN 客户端与 WLAN 服务端关联时选择采用 WAPI 安全机制，则必须进行相互身份鉴别和密钥协商。WAPI 提供两种身份鉴别和密钥管理方法：基于证书的方式（WAPI-CERT 方式）和基于预共享密钥的方式（WAPI-PSK 方式）。

**WAPI-CERT**：若采用基于证书的方式，整个过程包括证书鉴别、单播密钥协商和组播密钥通告。证书鉴别是基于 WLAN 客户端与 WLAN 服务端双方的证书所进行的鉴别。鉴别前 WLAN 客户端与 WLAN 服务端必须预先拥有各自的证书，然后通过 ASU 对双方的身份进行鉴别，根据双方产生的临时公钥和临时私钥生成 BK（基密钥），并为随后的单播密钥协商和组播密钥通告做好准备。

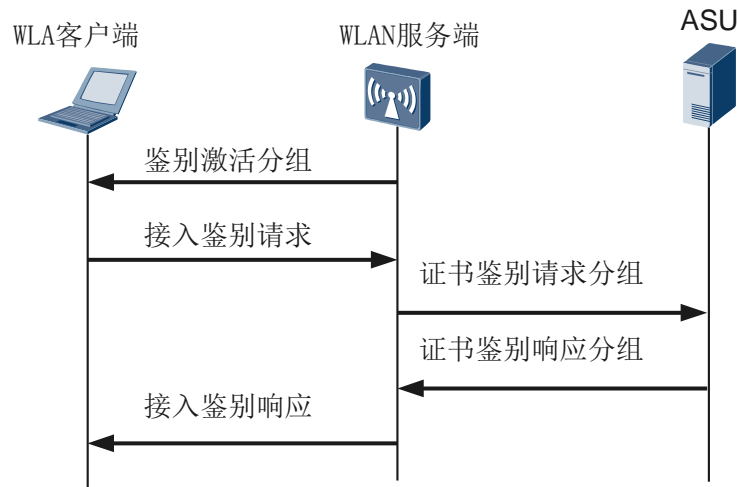
**WAPI-PSK**：若采用预共享密钥的方式，整个过程则为单播密钥协商与组播密钥通告。预共享密钥鉴别是基于 WLAN 客户端与 WLAN 服务端双方的预共享密钥所进行的鉴别。鉴别前 WLAN 客户端与 WLAN 服务端必须预先配置有相同的密钥，即预共享密钥。鉴别时直接将预共享密钥转换为 BK（基密钥），然后进行单播密钥协商和组播密钥通告。在单播密钥协商和组播密钥通告成功之后，WLAN 客户端与 WLAN 服务端才可以开始数据传输，数据传输时使用协商出来的密钥对它们之间的数据进行加解密，加密算法采用 WPISMS4

### 说明

WAPI-PSK 一般适合家庭用户或小型企业网络中，WAPI-CERT 适用于大型企业网络或运营商网络，这种认证方式需要部署和维护昂贵的证书系统。

- WAPI 证书鉴别

图1-8 WAPI 证书鉴别



如图 1-8 所示，WAPI 证书鉴别流程如下：

1. 鉴别激活：当 WLAN 客户端关联或重新关联至 WLAN 服务端时，由 WLAN 服务端向 WLAN 客户端发送鉴别激活以启动整个鉴别过程。
2. 接入鉴别请求：WLAN 客户端向 WLAN 服务端发出接入鉴别请求，将 WLAN 客户端证书与 WLAN 客户端的当前系统时间发往 WLAN 服务端，其中系统时间称为接入鉴别请求时间。
3. 证书鉴别请求：WLAN 服务端收到 WLAN 客户端接入鉴别请求后，首先记录鉴别请求时间，然后向 ASU 发出证书鉴别请求，即将 WLAN 客户端证书、接入鉴别请求时间、WLAN 服务端证书及使用 WLAN 服务端的私钥对它们的签名构成证书鉴别请求发送给 ASU。
4. 证书鉴别响应：ASU 收到 WLAN 服务端的证书鉴别请求后，验证 WLAN 服务端的签名和 WLAN 服务端证书的有效性，若不正确，则鉴别过程失败，否则进一步验证 WLAN 客户端证书。验证完毕后，ASU 将 WLAN 客户端证书鉴别结果信息、WLAN 服务端证书鉴别结果信息和 ASU 对它们的签名构成证书鉴别响应发送给 WLAN 服务端。
5. 接入鉴别响应：WLAN 服务端对 ASU 返回的证书鉴别响应进行签名验证，得到 WLAN 客户端证书的鉴别结果，根据此结果对 WLAN 客户端进行接入控制。WLAN 服务端将收到的证书鉴别响应回送至 WLAN 客户端。WLAN 客户端验证 ASU 的签名后，得到 WLAN 服务端证书的鉴别结果，根据该鉴别结果决定是否接入该 WLAN 服务。

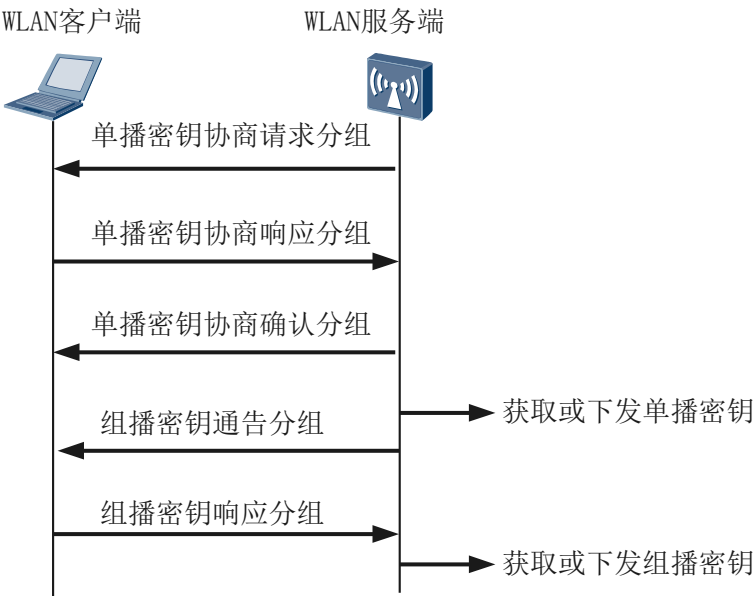
至此 WLAN 客户端与 WLAN 服务端之间完成了证书鉴别过程。若鉴别成功，则 WLAN 服务端允许 WLAN 客户端接入，否则解除其关联。

- WAPI 密钥协商

WLAN 客户端与 WLAN 服务端之间交互的单播数据利用单播密钥协商过程所协商出的单播加密密钥和单播完整性校验密钥进行保护；WLAN 服务端利用自己通告的、由组播主密钥导出的组播加密密钥和组播完整性校验密钥对其发送的广播/组播数据进行保护，而 WLAN 客户端则采用 WLAN 服务端通告的、由组播主密钥导出的组播加密密钥和组播完整性校验密钥对收到的广播/组播数据进行解密。

为了进一步提高通信的保密性，在通信一段时间或交换一定数量的数据之后，WLAN 客户端与 WLAN 服务端之间可以重新进行会话密钥的协商。

图1-9 WAPI 密钥协商



如图 1-9 所示，具体步骤说明如下：

1. 单播密钥协商

单播密钥协商在证书鉴别并且已生成 BK 的基础上，利用 BK、WLAN 客户端质询、WLAN 服务端质询，采用算法 KD-HMAC-SHA256 生成单播会话密钥 USK。单播密钥协商过程不仅要协商出 WLAN 客户端和 WLAN 服务端会话时单播数据的加密密钥，而且还要协商出会话过程所使用的组播密钥的保护密钥和鉴别密钥。

– 单播密钥协商请求分组

建立有效的基密钥安全关联后，WLAN 服务端向 WLAN 客户端发送单播密钥协商请求分组，开始与 WLAN 客户端进行单播密钥协商。

– 单播密钥协商响应分组

WLAN 客户端收到 WLAN 服务端的单播密钥协商请求分组后，进行如下处理：

- a. 检查此次单播密钥协商是否为更新过程，如果是执行步骤 b，否则执行步骤 c。
- b. 检查 WLAN 服务端质询与本地保存的上次单播密钥协商过程所协商的质询是否相同，如果不同，丢弃分组。
- c. WLAN 客户端生成随机数质询，利用基密钥、WLAN 服务端随机数质询、WLAN 客户端随机数质询，采用密钥导出算法 KD-HMAC-SHA256，生成单播会话密钥和下次单播密钥协商过程的 WLAN 服务端质询。
- d. 用消息鉴别密钥通过 HMAC-SHA256 算法本地计算消息鉴别码，构造单播密钥协商响应分组发送给 WLAN 服务端。

WAI 密钥管理协议也允许 WLAN 客户端直接发送单播密钥协商响应分组给 WLAN 服务端，主动发起单播密钥更新过程。

– 单播密钥协商确认分组

WLAN 服务端收到单播密钥协商响应分组后，进行如下处理：

- a. 检查 WLAN 服务端质询是否正确，如果不正确，丢弃分组。
- b. 利用基密钥、WLAN 服务端质询、WLAN 客户端质询，采用密钥导出算法 KD-HMAC-SHA256，生成单播会话密钥和下次单播会话密钥协商过程的 WLAN 服务端质询，利用消息鉴别密钥通过 HMAC-SHA256 算法本地计算消息鉴别码，与分组中的消息鉴别码比较，如果不同，丢弃分组。
- c. 如果为基密钥安全关联建立后的首次单播密钥协商，在基础模式下，检查响应分组中的 WAPI 信息元素和自己收到的关联请求帧的 WAPI 信息元素是否相同，如果不同，解除认证。在 IBSS 模块下，检查响应分组中的 WAPI 信息元素中的单播密钥算法是否支持，如果不支持，解除认证。
- d. 用消息鉴别密钥通过 HMAC-SHA256 算法本地计算消息鉴别码，构造单播密钥协商确认分组，发送给 WLAN 客户端。

2. 组播密钥通告

组播密钥通告过程建立在单播密钥协商过程上，完成 WLAN 服务端组播密钥的通告：

– 组播密钥通告分组

单播密钥协商成功后，WLAN 服务端将组播主密钥（利用随机数算法生成的），利用前面协商出的单播密钥对组播密钥进行加密，发送组播密钥通告分组，向 WLAN 客户端通告组播密钥。

– 组播密钥响应分组

WLAN 客户端收到组播密钥通告分组后，进行如下处理：

- a. WLAN 客户端利用单播密钥标识字段标识的消息鉴别密钥计算校验和，与消息鉴别码字段进行比较，如果不同，丢弃分组。
- b. 检查密钥通告标识字段值是否单调递增，如果不是，丢弃分组。
- c. 对密钥数据解密得到 16 个八位位组的通告主密钥，利用 KD-HMAC-SHA256 算法进行扩展，生成长度位 32 个八位位组的会话密钥（其中前 16 个八位位组位加密密钥，后 16 个八位位组位完整性校验密钥）。
- d. 保存密钥通告标识字段值，生成组播密钥响应分组发送给 WLAN 服务端。

WLAN 服务端收到 WLAN 客户端的组播密钥响应分组后，进行如下处理：

- a. 利用单播密钥标识字段标识的消息鉴别密钥计算校验和，与消息鉴别码字段进行比较，如果不同，丢弃分组。
- b. 比较密钥通告标识等字段与发送的组播密钥通告分组中的相应字段值，如果都相同，则本次组播密钥通告成功，否则丢弃分组。

如果此次组播密钥通告过程为基密钥安全关联建立后的首次通告过程，则将受控端口状态置为 On。



说明

WAPI 服务与 WEP/WPA/WPA2 的区别：



- WAPI 支持 WLAN 客户端和接入网络的双向认证，即网络验证用户的合法性，用户也可以验证接入网络的合法性。
- WAPI-CERT 采用证书认证方式，证书认证过程采用公钥算法，WLAN 客户端和 WLAN 服务端需要部署证书。
- WAPI 认证虽然使用非对称加密算法，但对无线数据的加密仍使用对称加密算法，主要是基于加解密效率和软硬件实现复杂度方面的考虑。

## WAPI 的认证加密组合

- WAPI 证书鉴别方式

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wapi
[Quidway-wlan-sec-prof-huawei] wapi authentication-method certificate
[Quidway-wlan-sec-prof-huawei] wapi asu ip 10.10.10.1
[Quidway-wlan-sec-prof-huawei] wapi import certificate ac file-name
flash:/huawei-ac.cer
[Quidway-wlan-sec-prof-huawei] wapi import certificate asu file-name
flash:/huawei-asu.cer
[Quidway-wlan-sec-prof-huawei] wapi import certificate issuer file-name
flash:/huawei-asu.cer
[Quidway-wlan-sec-prof-huawei] wapi import private-key file-name flash:/huawei-
ac.cer
```

- WAPI 预共享密钥鉴别方式

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wapi
[Quidway-wlan-sec-prof-huawei] wapi authentication-method psk pass-phrase
simple 01234567
```

## Portal 认证

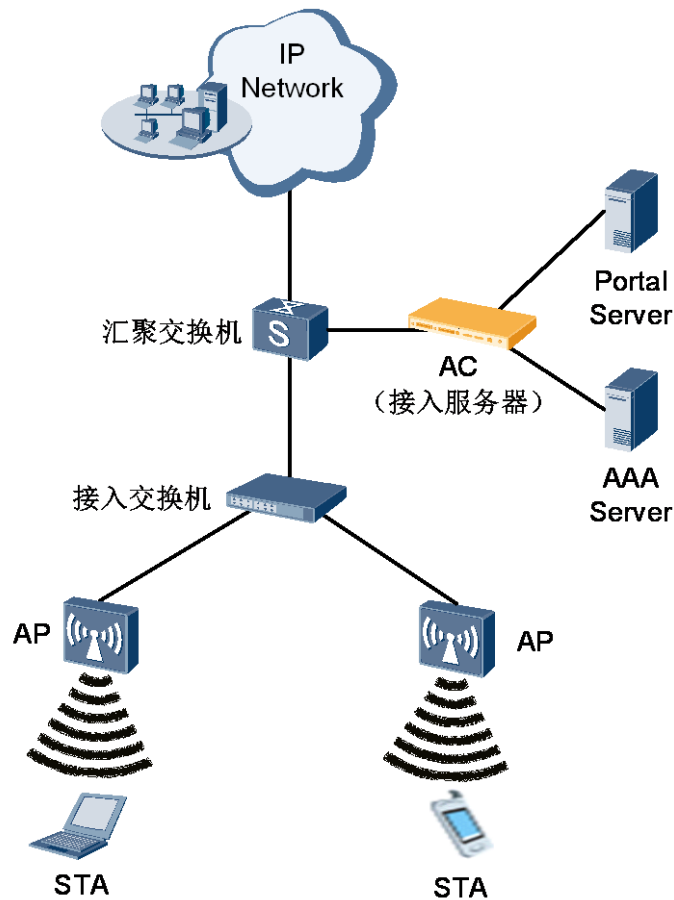
Portal 认证即 WEB 认证。用户通过主动访问位于 Portal 服务器上的认证页面（主动认证），或用户试图通过 HTTP 访问其他外网被 WLAN 服务端强制重定向到 WEB 认证页面后（强制认证），输入用户帐号信息，提交 WEB 页面后，Portal 服务器获取用户帐号信息。Portal 服务器通过 Portal 协议与 WLAN 服务端交互，将用户帐号信息发送给 WLAN 服务端，服务端与认证服务器交互完成用户认证过程。

Portal 认证可以提供方便的管理功能，开展广告、社区服务、个性化的业务等，使运营商、设备提供商和内容服务提供商形成一个产业生态系统。Portal 认证在 WLAN 运营网和企业网中大量使用。

Portal 认证通常由 4 个基本要素组成：客户端、接入服务器、Portal 服务器、AAA 服务器，具体组网如图 1-10 所示，AC 担当接入服务器。

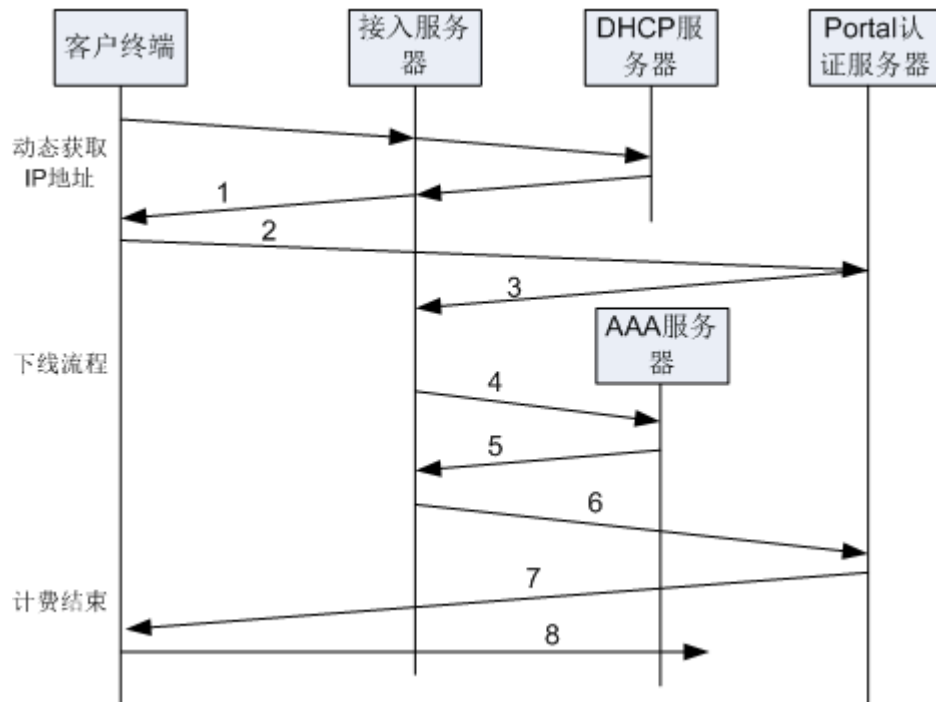


图1-10 Portal 认证系统组网图



Portal 的认证方式分为 2 种：二层认证方式和跨三层认证方式。二层认证用户和跨三层认证用户的区别在于用户 MAC 地址接入服务器无法获取，因而不能进行 MAC、IP 的绑定检查，安全性相对较差；ARP 请求不能穿透路由器，不能对用户进行 ARP 探测确定是否在线。二层认证和可跨三层认证的流程一样，具体如图 1-11 所示：

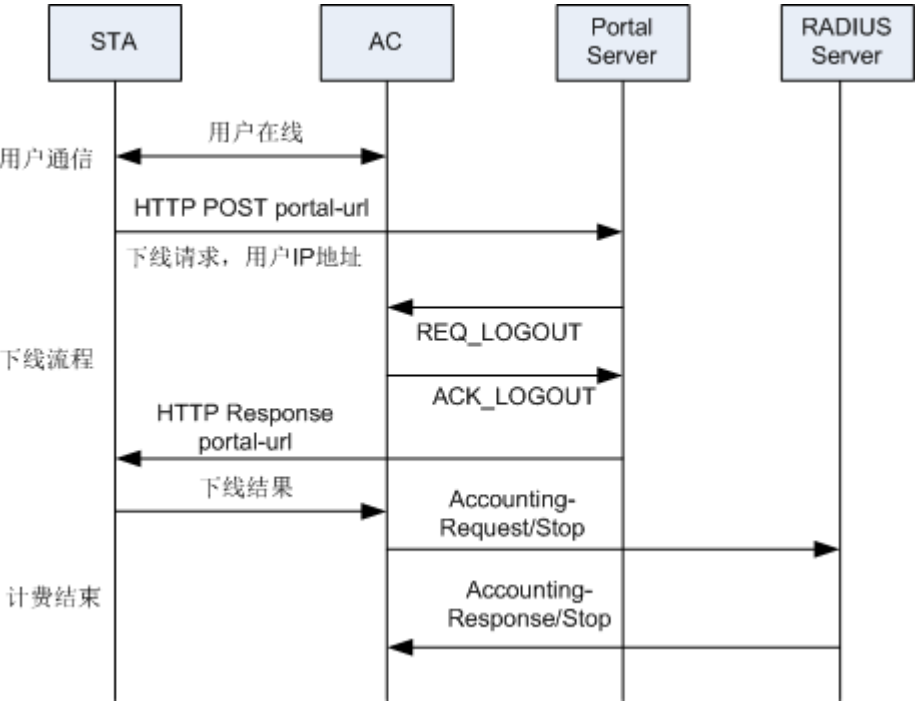
图1-11 Portal 认证系统组网图



1. 动态用户通过 DHCP 协议获取地址的过程（静态用户手工配置地址即可。）。
2. 用户访问 Portal 认证服务器的认证页面，并在其中输入用户名、密码，点击登陆按钮。
3. Portal 认证服务器将用户的信息通过内部协议，通知接入服务器。
4. 接入服务器到相应的 AAA 服务器对该用户进行认证。
5. AAA 服务器返回认证结果给接入服务器。
6. 接入服务器将认证结果通知 Portal 认证服务器。
7. Portal 认证服务器通过 HTTP 页面将认证结果通知用户。
8. 如果认证成功用户即可正常访问网络资源。

Portal 认证用户下线包括用户主动下线和异常下线两种情况。

图1-12 用户主动下线流程



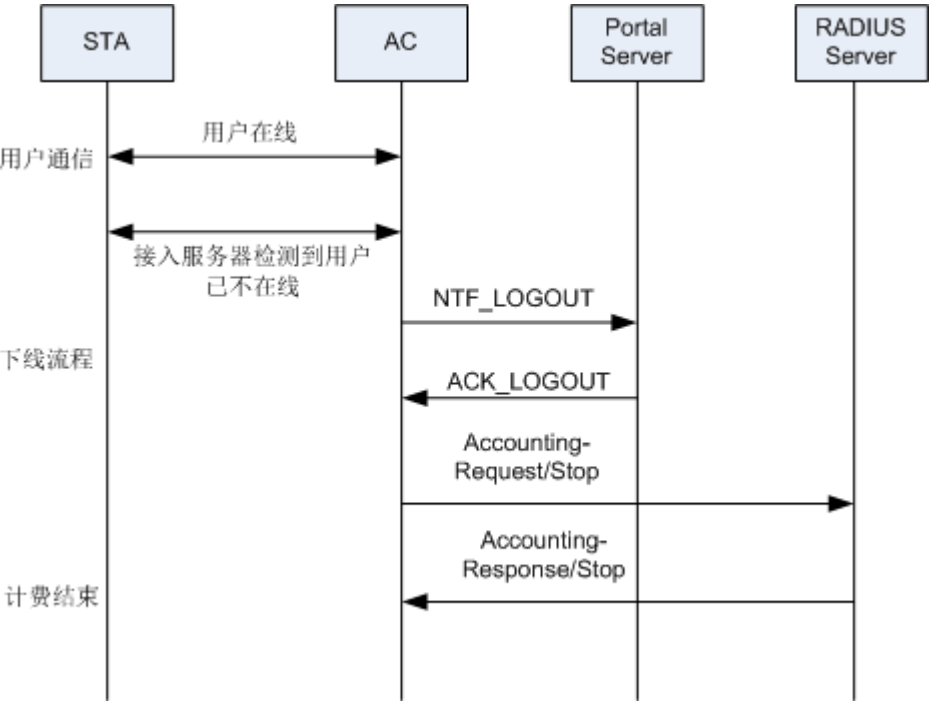
用户主动下线流程如图 1-12 所示：

1. 当用户需要下线时，可以点击认证结果页面上的下线机制，向 Portal 服务器发起一个下线请求。
2. Portal 服务器向 AC 发起下线请求。
3. AC 返回下线结果给 Portal 服务器。
4. Portal 服务器根据下线结果，推送含有对应的信息的页面给用户。
5. 当 AC 收到下线请求时，向 RADIUS 服务器发计费结束报文。
6. RADIUS 服务器回应 AC 的计费结束报文。

异常下线：

AC 检测到用户下线，流程如图 1-13 所示：

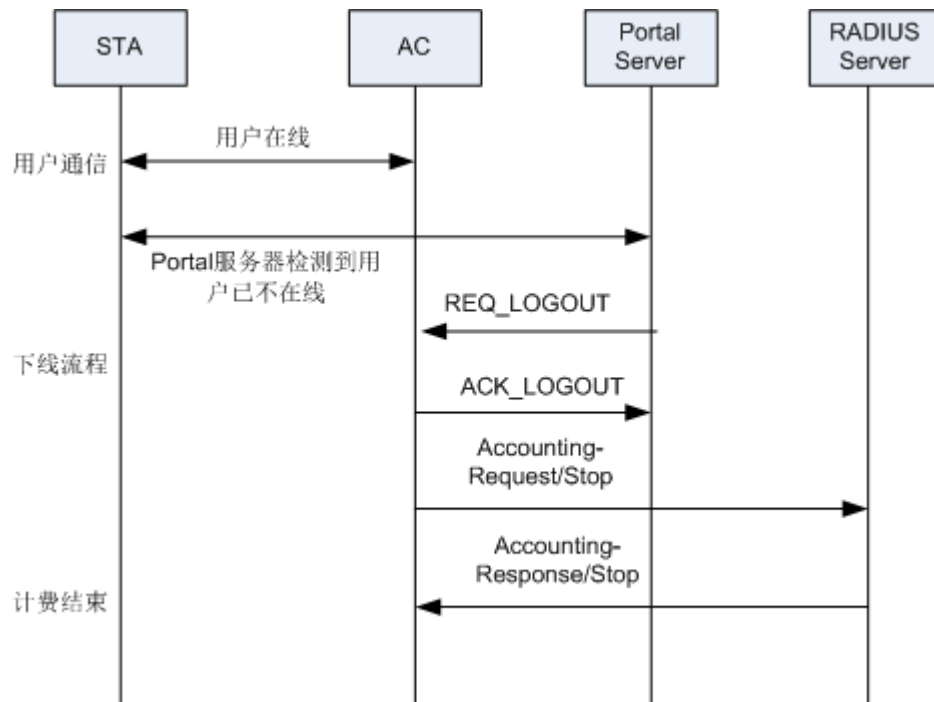
图1-13 AC 检测到用户异常下线流程



1. AC 检测到用户下线，向 Portal 服务器发出下线请求。
2. Portal 服务器回应下线成功。
3. 当 AC 收到 Portal 服务器的下线成功消息时，向 RADIUS 用户认证服务器发计费结束报文。
4. RADIUS 用户认证服务器回应 AC 的计费结束报文。

Portal 服务器检测到用户下线，流程如图 1-14 所示：

图1-14 Portal 服务器检测到用户异常下线流程



1. Portal 服务器检测到用户下线，向 AC 发出下线请求。
2. AC 回应下线成功。
3. 当 AC 收到下线请求时，向 RADIUS 用户认证服务器发计费结束报文。
4. RADIUS 用户认证服务器回应 AC 的计费结束报文。

## MAC 认证

MAC 认证是另外一种接入认证方式。MAC 接入认证主要为客户端以自己的 MAC 地址作为身份凭据到设备端进行认证。

MAC 认证也使用 RADIUS 服务器对客户端进行认证。当服务端获取客户端的 MAC 地址后，会主动向 RADIUS 服务器发起认证请求。RADIUS 服务器完成对该客户端的认证，并通知服务端认证结果以及相应的授权信息。MAC 认证过程不需要客户端参与，也不需要安装客户端软件。

MAC 认证除了实现 MAC 地址认证外，还可以实现对该用户的计费和授权。

### 1.2.4 数据加密技术

保护无线链路数据的私密性，是所有无线网络均需要面对的挑战。与有线网络不同，只要持有适当的接收设备，任何人都可以被动监听帧且加以分析。

为了避免数据沦落到“不对的”人手中，必须对数据进行加密，防止数据被攻击者取得。WLAN 提供了一系列的加密协议，只允许拥有密钥的授权用户访问数据，同时确保数据在传输过程中未遭篡改。

无线局域网 WLAN 能够使用的加密协议如下：

- WEP
- 临时密钥完整性协议(TKIP)
- CBC-MAC 计数模式协议 (CCMP)
- SMS4 算法
- 网络层加密协议

## WEP 加密

WEP 是 802.11 最早的安全标准，称为有线等效私密性（WEP，Wired Equivalent Privacy）。WEP 安全措施主要包括两部分：先是认证阶段，然后是加密阶段。WEP 是 802.11 最早的安全标准，称为有线等效私密性 WEP（Wired Equivalent Privacy）。WEP 安全措施主要包括两部分：先是认证阶段，然后是加密阶段。当一个新的移动点想加入接入点，它必须首先证明自己的身份。认证过程结束后，进行数据的加密传输，数据加密算法采用 RC4 算法。

WEP 认证过程请参考 [1.2.2 STA 身份验证](#) 中的“共享密钥认证过程”。

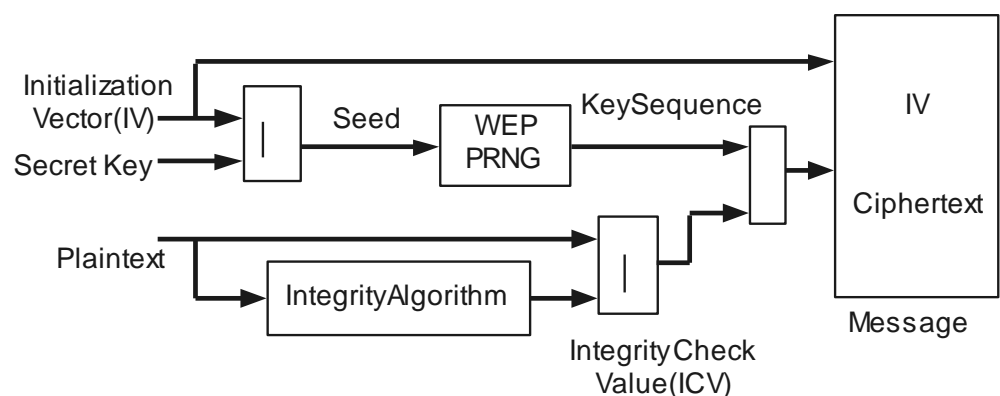
## 静态 WEP 加密

在 IEEE802.11 中，定义了 WEP 对无线数据进行加密，WEP 的核心是采用 RC4 算法。在标准中，加密密钥长度有 64 位和 128 位两种。其中有 24Bit 的 IV 是由系统产生的，在 WLAN 服务端和 WLAN 客户端上配置的密钥就需要 40 位或 104 位。

802.11 并未规范 WEP 必须使用的特定密钥分配机制。早期的 WEP 实现必须手动分配密钥，手动更新密钥。而更新密钥对于网管而言是莫大的负担，所以大多数的网络都会被部署成长时间使用同一个密钥。这种不具备密钥分配机制的 WEP 通常称为手动 WEP 或者静态 WEP。

静态 WEP 是迫不得已才会使用的加密协议，唯一可以考虑的场景是：部分老式低功率终端，如手持条码扫描器、PDA、WIFI 电话等，当他们不能支持更高级的加密协议时，就只能采用这种静态 WEP。

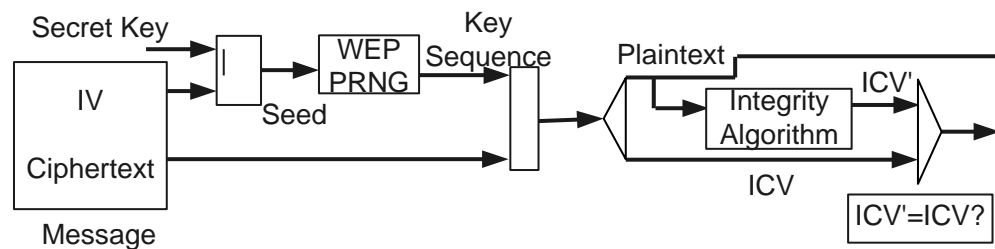
图1-15 WEP 加密原理图



如图 1-15 所示，WEP 加密过程如下：

1. WLAN 服务端先产生一个 IV，将其同密钥串接（IV 在前）作为 WEP Seed，采用 RC4 算法生成和待加密数据等长（长度为 MPDU 长度加上 ICV 的长度）的密钥序列；
2. 计算待加密的 MPDU 数据校验值 ICV，将其串接在 MPDU 之后；
3. 将上述两步的结果按位异或生成加密数据；
4. 加密数据前面有四个字节，存放 IV 和 Key ID，IV 占前三个字节，Key ID 占第四字节的高两位，其余的位置为 0；如果用 Key-mapping Key，则 Key ID 为 0，如果用 Default Key，则 Key ID 为密钥索引（取值范围 0-3）。

图1-16 WEP 解密原理图



如图 1-16 所示，WEP 解密过程如下：

1. 找到解密密钥；
2. 将密钥和 IV 串接（IV 在前）作为 RC4 算法的输入生成和待解密数据等长的密钥序列；
3. 将密钥序列和待解密数据按位异或，最后 4 个字节是 ICV，前面是数据明文；
4. 对数据明文计算校验值 ICV'，并和 ICV 比较，如果相同则解密成功，否则丢弃该数据。

### WEP 缺点

- WEP 是一种在接入点和客户端之间以“RC4”方式对分组信息进行加密的技术，密钥一旦设置，就无法自动更新。并且在传输中密码很容易被破解，目前网络上已经有大量针对 WEP 加密的解密方法介绍。具体原因如下：  
WEP 使用的加密密钥包括：收发双方预先确定的 40 位（或者 104 位）通用密钥和发送方为每个分组信息所确定的 24 位、被称为 IV 密钥的加密密钥。从加密原理框图可以看出，为了将 IV 密钥告诉给通信对象，IV 密钥不经加密就直接嵌入到分组信息中被发送出去。如果通过无线窃听，收集到包含特定 IV 密钥的分组信息并对其进行解析，那么就连秘密的通用密钥都可能被计算出来。
- 没有消息完整性校验，信息容易被黑客篡改。
  - 加密原理框图中 ICV 的目的是为了保证数据在传输途中不会因为噪声等物理因素导致报文出错，因此采用相对简单高效的 CRC 算法，但是黑客可以通过修改 ICV 值来使之和被篡改过的报文相吻合，可以说没有任何安全的功能。
  - WEP 还缺乏认证手段，无法确认用户凭证，这难以保证接入网络的用户都是合法的。

## 802.1X 动态 WEP 加密

比静态 WEP 好的安全解决方案是动态 WEP。在动态 WEP 中，每个 STA 会使用两个密钥，而不是所有 STA 共享同一个密钥。其中私有密钥用来保护单播帧，共享密钥用来保护广播和组播帧。而且动态密钥本身可以随时间而改变，这样也可以提高保护密钥的强度。

虽然 802.1X 是设计来做身份验证的，它对 WEP 的改良也同等总要。802.1X 所包含的信息可以用来将密钥从认证点（胖 AP 或 AC）传递给 STA。

动态 WEP 充其量只是过渡时期的解决方案，除非设备不支持 TKIP，否则不应使用。使用动态 WEP 时切忌将密钥使用时间缩短，建议时间不超过 15 分钟，以防 WEP 分析工具的攻击。

## WPA/WPA2: TKIP&CCMP 加密

WPA 是 Wi-Fi 保护存取（Wi-Fi Protected Access）的缩写，是由 Wi-Fi 联盟所推行的商业标准，由于早期的 WEP 认证和加密被证明很不安全，市场急需推出一个可以代替 WEP 的替代品，在 802.11i 安全标准没有正式推出前，Wi-Fi 组织推出了针对 WEP 改良的认证方法，就是 WPA，针对 WEP 的各种缺陷做了改进，核心的数据加密算法仍然采用 RC4 算法，称为 TKIP（Temporal Key Integrity Protocol）加密算法。

随着 802.11i 安全标准的正式推出，推出了 WPA2，有别于 WPA，WPA2 采用了 802.1X 的身份验证框架，支持的认证方式有 EAP-PEAP、EAP-TLS 等。由于每次产生的密钥种子（PMK）不一样，由种子衍生出来的数据加密密钥理论上就很安全，因为用户每次上线过程中，种子的产生是不一样的。WPA2 采用计数器模式及密码块链消息认证码协议 CCMP（CTR with CBC-MAC Protocol）加密算法进行数据加密。

在最新的实现中，不管是 WPA1 还是 WPA2 都可以使用 802.1X、TKIP 或者 CCMP 进行加密，他们之间的不同表现主要在协议报文格式上，而安全性上几乎没有差别。

在 IEEE 802.11i 标准最终确定前，WPA 标准是代替 WEP 的无线安全标准协议，为 IEEE 802.11 无线局域网提供更强大的安全性能。WPA 是 IEEE802.11i 的一个子集，其核心就是 IEEE802.1x 和 TKIP。

WPA/WPA2 作为 IEEE 802.11 通用的加密机制 WEP 的升级版，在安全的防护上比 WEP 更为周密，主要体现在身份认证、数据加密和完整性校验等方面，而且它还提升了无线网络的管理能力。

- 身份认证

在 802.11 中几乎形同虚设的认证阶段，到了 WPA 中变得尤为重要起来，它强制用户必须提供身份凭据来证明它是合法用户，并拥有对某些网络资源的访问权。

WPA 的认证分为两种版本：WPA 企业版和 WPA 个人版。

- WPA 企业版：是指采用 WPA-802.1X 的方式，用户提供认证所需的凭证，如用户名密码，通过特定的用户认证服务器（一般是 RADIUS 服务器）来实现。
- WPA 个人版：对一些中小型企业网络或者家庭用户，架设一台专用的认证服务器未免代价过于昂贵，维护也很复杂，因此 WPA 也提供一种简化的模式，即 WPA 预共享密钥(WPA-PSK)模式，它不需要专门的认证服务器，仅要求在每个 WLAN 节点(AP、AC、网卡等)预先输入一个预共享密钥即可。只要密钥吻合，客户就可以获得 WLAN 的访问权。由于这个密钥仅仅用于认证过程，



而不用加密过程，因此不会导致诸如使用 WEP 密钥来进行 802.11 共享认证那样严重的安全问题。



说明

在大型企业网络中，通常采用 WPA 企业版的认证方式。

IEEE 802.11i 的新一代安全标准为了增强 WLAN 的数据加密和认证性能，定义了固安网络 RSN（Robust Security Network）的概念，并且针对 WEP 加密机制的各种缺陷做了多方面的改进：

- 增强了 STA 和 AP 的认证机制
  - 支持 802.1x 认证方式
  - 支持 Pre-shared key 认证方式
- 增加了 Key 的生成、管理以及传递的机制
  - 每用户使用独立的 Key
  - 通过安全的传递方法传递用户数据加密使用的 Key
- 增加了两类对称加密算法，加密强度大大增强
  - TKIP：其中 TKIP 采用 WEP 机制里的 RC4 作为核心加密算法，可以通过在现有的设备上升级固件和驱动程序的方法达到提高 WLAN 安全的目的。
  - CCMP：核心为 AES（Advanced Encryption Standard，先进加密标准）算法，由于 AES 对硬件要求比较高，因此 CCMP 无法通过在现有设备的基础上进行升级实现。
  - WRAP：WRAP 机制基于 AES 加密算法和 OCB（Offset Codebook），是一种可选的加密机制。

## TKIP

802.11i 为了解决 WEP 在设计商的主要瑕疵，修正了链路层加密协议，解决了 WEP 加密机制缺乏机密性的问题。第一种称为 TKIP，被设计来尽可能强化 pre-802.11i 硬件的安全性。另一种则是重新打造的加密协议，称为 CCMP，被设计来提供最高等级的安全性。

TKIP 原本称为“WEP2”，当 WEP 最后被证明存在瑕疵时，此协议就更名为“TKIP”，以便与 WEP 有所区别。

WEP 的主要破绽在于其随机数种子是由初始向量 IV 和 WEP 密钥所构成。为了防范对初始向量的攻击，TKIP 将 IV 的长度由 24bit 增为 48bit，极大的提升了初始向量的空间。TKIP 同时以密钥混合的方式来防范针对 WEP 的攻击。在 TKIP 中，各个帧均会被特有的 RC4 密钥加密，更进一步扩展了初始向量的空间。

TKIP 加密实际上是增强了 WEP，核心算法采用 RC4。TKIP 相对于 WEP 增加了 EIV(扩展 IV)和 MIC。作用是防止重放攻击、信息篡改。

TKIP（WEP2）是 IEEE802.11i 工作组提出的对 WEP 的改进技术。该技术对 WEP 进行的改进点包括：

1. 发送端计算信息完整码（MIC，Message Integrity Check），保护信息的完整性。计算 MIC 时，除了包括明文还包括源和目的地址。计算结果还用 MIC 密钥加密。

2. 使用数据包序列号防止重放攻击，序列号放在 WEP 初始向量中。
3. 使用 Fast Packet Keying 算法将临时密钥和包序列号混合，生成包加密密钥。
4. 使用 802.1x EAPoL Key 协议更新临时和 MIC 密钥。

TKIP 的优点：

1. TKIP 能够在一定程度上防止 MAC 地址被盗用。使用 TKIP 并没有对 MAC 地址提供额外的保护，也就是加密不包括对 MAC 地址的加密，窃听者仍然可以窃听到 MAC 地址。但是窃听者取得他人的 MAC 地址后，不能在 TKIP 中正常使用，因为 TKIP 通过消息完整性保护码提供对消息源的验证，发送者必须有 MIC KEY 才能够计算出正确的 MIC。
2. 能够提供对源地址和目的地址的保护。源地址（SA）和目的地址（DA）如果在传输中被改动，TKIP 也是能够检测出来的。因为 MIC 是基于 SA，DA，和 MIC KEY。如果 DA，SA 被改动，那么接收端计算的 MIC 与收到的 MIC 是不会相同的。
3. 能够提供防重播的保护，TKIP 中 TSC（序列号）能够提供防重播的保护，TSC 对于每个 MSDU（数据分组）都是不同的，且序号递增，这样能够防止攻击者窃听某些消息后，根据消息的内容给接收者发送信息。
4. 能够防止攻击者对加密的信息分析猜出密钥。对 WEP 中密钥和 IV 矢量的组合是使用了新的混合函数。而不是 WEP 中密钥和 IV 的简单的连接混合。TKIP 中增加了序列号 TSC 作为混合函数的输入，也增强了密钥的安全。

## CCMP 加密

TKIP 比 WEP 优秀，但其仍然以流密码为基础，无法摆脱人们对其安全性的怀疑。

IEEE 工作组开发了以高级加密标准（AES）的块密码为基础的安全协议。802.11i 规定 AES 使用 128bit 的密钥和 128bit 的数据块。

这个以 AES 为基础的链路层安全协议称为 Counter Mode with CBC-MAC Protocol (简称 CCMP)。

CCMP 提供了加密、认证、完整性和重放保护功能。CCMP 是基于 CCM 方式的，该方式使用了 AES(Advanced Encryption Standard)加密算法。CCM 方式结合了用于加密的 CTR（Counter Mode）和用于认证和完整性加密块链接消息的认证码 CBC-MAC（Cipher Block Chaining Message Authentication Code）。CCM 保护 MPDU 数据和 IEEE802.11 MPDU 帧头部分域的完整性。

同样 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），保证每一个加密报文都会是用不同的 PN，在一定程度上提高安全性。

CCMP 的优点：

1. 在 WLAN 底层引入 AES 算法，即加密和解密一般由硬件完成，克服 WEP 的缺陷，有线对等保密(WEP)协议的缺陷延缓了无线局域网(WLAN)在许多企业内的应用和普及。无线局域网网络会暴露某个网络，因此，从安全的角度来讲，不能像核心企业网络而必须像接入网络那样来对待。如果企业用户通过一个局域网交换中心互相连接，人们就可认为他们已经成为信任用户。

## 2. 克服了 RC4 的天然不足：

- RC4 算法本身的缺陷，在接入点和客户端之间以“RC4”方式对分组信息进行加密的技术，密码很容易被破解。

无论是 WEP 加密还是 TKIP 加密都是以 RC4 算法为核心，由于 RC4 算法本身的缺陷，在接入点和客户端之间以“RC4”方式对分组信息进行加密的技术，密码很容易被破解。AES 是一种对称的块加密技术，提供比 WEP/TKIP 中 RC4 算法更高的加密性能。对称密码系统要求收发双方都知道密钥，而这种系统的最大困难在于如何安全地将密钥分配给收发的双方，特别是在网络环境中，IEEE 802.11 体系使用 802.11 认证和密钥协商机制来管理密钥。AES 加密算法使用 128bit 分组加密数据。它的输出更具有随机性，对 128 比特、轮数为 7 的密文进行攻击时需要几乎整个的密码本，对 192、256 比特加密的密文进行攻击不仅需要密码本，还需要知道相关的但并不知道密钥的密文，这比 WEP 具有更高的安全性，攻击者要获取大量的密文，耗用很大的资源，花费更长的时间破译。它解密的密码表和加密的密码表是分开的，支持子密钥加密，这种做法优于最初的用一个特殊的密钥解密，很容易防护暴力攻击和同步攻击，加密和解密的速度快，在安全性上优于 WEP。

- AES 是一种对称的块加密技术，使用 128 位的密钥和 128 位的块大小。攻击者要获取大量的密文，耗用更多的资源，花费更长的时间来破译。

AES 算法支持任意分组的大小，密钥的大小为 128、192、256，可以任意组合。此外，AES 还具有应用范围广、等待时间短、相对容易隐藏、吞吐量高的优点。经过比较分析，可知此算法在性能等各方面都优于 WEP 和 TKIP，利用此算法加密，无线局域网的安全性会获得大幅度提高，从而能够有效地防御外界攻击。

WPA 认证加密支持下列组合方式：

- WPA-PSK+TKIP，具体配置如下：

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa
[Quidway-wlan-sec-prof-huawei] wpa authentication-method psk pass-phrase simple
01234567 encryption-method tkip
```

- WPA-PSK+CCMP，具体配置如下：

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa
[Quidway-wlan-sec-prof-huawei] wpa authentication-method psk pass-phrase simple
01234567 encryption-method ccmp
```

- WPA2-PSK+TKIP，具体配置如下：

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa2
[Quidway-wlan-sec-prof-huawei] wpa2 authentication-method psk pass-phrase
simple 01234567 encryption-method tkip
```

- WPA2-PSK+CCMP，具体配置如下：

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa2
[Quidway-wlan-sec-prof-huawei] wpa2 authentication-method psk pass-phrase
simple 01234567 encryption-method ccmp
```

- WPA-802.1X+PEAP+TKIP，具体配置如下：

```
<Quidway> system-view
[Quidway] radius-server template radius_huawei
[Quidway-radius-radius_huawei] radius-server authentication 10.138.18.152 1812
[Quidway-radius-radius_huawei] radius-server accounting 10.138.18.152 1813
[Quidway-radius-radius_huawei] radius-server shared-key simple huawei
[Quidway-radius-radius_huawei] quit
[Quidway] aaa
[Quidway-aaa] authentication-scheme radius_huawei
[Quidway-aaa-authen-radius_huawei] authentication-mode radius
[Quidway-aaa-authen-radius_huawei] quit
[Quidway-aaa] accounting-scheme radius_huawei
[Quidway-aaa-accounting-radius_huawei] accounting-mode radius
[Quidway-aaa-accounting-radius_huawei] quit
[Quidway-aaa] domain peap.radius.com
[Quidway-aaa-domain-peap.radius.com] authentication-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] accounting-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] radius-server radius_huawei
[Quidway-aaa-domain-peap.radius.com] quit
[Quidway-aaa] quit
[Quidway] interface wlan-ess 0
[Quidway-Wlan-Ess0] dot1x-authentication enable
[Quidway-Wlan-Ess0] dot1x authentication-method eap
[Quidway-Wlan-Ess0] force-domain huawei
[Quidway-Wlan-Ess0] peimit-domain huawei
[Quidway-Wlan-Ess0] quit
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa
[Quidway-wlan-sec-prof-huawei] wpa authentication-method dot1x peap encryption-
method tkip
```

- WPA-802.1x+PEAP+CCMP，具体配置如下：

```
<Quidway> system-view
[Quidway] radius-server template radius_huawei
[Quidway-radius-radius_huawei] radius-server authentication 10.138.18.152 1812
[Quidway-radius-radius_huawei] radius-server accounting 10.138.18.152 1813
[Quidway-radius-radius_huawei] radius-server shared-key simple huawei
[Quidway-radius-radius_huawei] quit
[Quidway] aaa
[Quidway-aaa] authentication-scheme radius_huawei
[Quidway-aaa-authen-radius_huawei] authentication-mode radius
[Quidway-aaa-authen-radius_huawei] quit
[Quidway-aaa] accounting-scheme radius_huawei
[Quidway-aaa-accounting-radius_huawei] accounting-mode radius
```

```
[Quidway-aaa-accounting-radius_huawei] quit
[Quidway-aaa] domain peap.radius.com
[Quidway-aaa-domain-peap.radius.com] authentication-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] accounting-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] radius-server radius_huawei
[Quidway-aaa-domain-peap.radius.com] quit
[Quidway-aaa] quit
[Quidway] interface wlan-ess 0
[Quidway-Wlan-Ess0] dot1x-authentication enable
[Quidway-Wlan-Ess0] dot1x authentication-method eap
[Quidway-Wlan-Ess0] force-domain huawei
[Quidway-Wlan-Ess0] peimit-domain huawei
[Quidway-Wlan-Ess0] quit
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa
[Quidway-wlan-sec-prof-huawei] wpa authentication-method dot1x peap encryption-
method ccmp
```

- WPA-802.1x+TLS+TKIP，具体配置如下：

```
<Quidway> system-view
[Quidway] radius-server template radius_huawei
[Quidway-radius-radius_huawei] radius-server authentication 10.138.18.152 1812
[Quidway-radius-radius_huawei] radius-server accounting 10.138.18.152 1813
[Quidway-radius-radius_huawei] radius-server shared-key simple huawei
[Quidway-radius-radius_huawei] quit
[Quidway] aaa
[Quidway-aaa] authentication-scheme radius_huawei
[Quidway-aaa-authen-radius_huawei] authentication-mode radius
[Quidway-aaa-authen-radius_huawei] quit
[Quidway-aaa] accounting-scheme radius_huawei
[Quidway-aaa-accounting-radius_huawei] accounting-mode radius
[Quidway-aaa-accounting-radius_huawei] quit
[Quidway-aaa] domain peap.radius.com
[Quidway-aaa-domain-peap.radius.com] authentication-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] accounting-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] radius-server radius_huawei
[Quidway-aaa-domain-peap.radius.com] quit
[Quidway-aaa] quit
[Quidway] interface wlan-ess 0
[Quidway-Wlan-Ess0] dot1x-authentication enable
[Quidway-Wlan-Ess0] dot1x authentication-method eap
[Quidway-Wlan-Ess0] force-domain huawei
[Quidway-Wlan-Ess0] peimit-domain huawei
[Quidway-Wlan-Ess0] quit
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa
[Quidway-wlan-sec-prof-huawei] wpa authentication-method dot1x tls encryption-
method tkip
```

- WPA-802.1x+TLS+CCMP，具体配置如下：

```
<Quidway> system-view
[Quidway] radius-server template radius_huawei
```

```
[Quidway-radius-radius_huawei] radius-server authentication 10.138.18.152 1812
[Quidway-radius-radius_huawei] radius-server accounting 10.138.18.152 1813
[Quidway-radius-radius_huawei] radius-server shared-key simple huawei
[Quidway-radius-radius_huawei] quit
[Quidway] aaa
[Quidway-aaa] authentication-scheme radius_huawei
[Quidway-aaa-authen-radius_huawei] authentication-mode radius
[Quidway-aaa-authen-radius_huawei] quit
[Quidway-aaa] accounting-scheme radius_huawei
[Quidway-aaa-accounting-radius_huawei] accounting-mode radius
[Quidway-aaa-accounting-radius_huawei] quit
[Quidway-aaa] domain peap.radius.com
[Quidway-aaa-domain-peap.radius.com] authentication-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] accounting-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] radius-server radius_huawei
[Quidway-aaa-domain-peap.radius.com] quit
[Quidway-aaa] quit
[Quidway] interface wlan-ess 0
[Quidway-Wlan-Ess0] dot1x-authentication enable
[Quidway-Wlan-Ess0] dot1x authentication-method eap
[Quidway-Wlan-Ess0] force-domain huawei
[Quidway-Wlan-Ess0] peimit-domain huawei
[Quidway-Wlan-Ess0] quit
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa
[Quidway-wlan-sec-prof-huawei] wpa authentication-method dot1x tls encryption-
method ccmp
```

- WPA2-802.1X+PEAP+TKIP，具体配置如下：

```
<Quidway> system-view
[Quidway] radius-server template radius_huawei
[Quidway-radius-radius_huawei] radius-server authentication 10.138.18.152 1812
[Quidway-radius-radius_huawei] radius-server accounting 10.138.18.152 1813
[Quidway-radius-radius_huawei] radius-server shared-key simple huawei
[Quidway-radius-radius_huawei] quit
[Quidway] aaa
[Quidway-aaa] authentication-scheme radius_huawei
[Quidway-aaa-authen-radius_huawei] authentication-mode radius
[Quidway-aaa-authen-radius_huawei] quit
[Quidway-aaa] accounting-scheme radius_huawei
[Quidway-aaa-accounting-radius_huawei] accounting-mode radius
[Quidway-aaa-accounting-radius_huawei] quit
[Quidway-aaa] domain peap.radius.com
[Quidway-aaa-domain-peap.radius.com] authentication-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] accounting-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] radius-server radius_huawei
[Quidway-aaa-domain-peap.radius.com] quit
[Quidway-aaa] quit
[Quidway] interface wlan-ess 0
[Quidway-Wlan-Ess0] dot1x-authentication enable
[Quidway-Wlan-Ess0] dot1x authentication-method eap
[Quidway-Wlan-Ess0] force-domain huawei
[Quidway-Wlan-Ess0] peimit-domain huawei
[Quidway-Wlan-Ess0] quit
```

```
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa2
[Quidway-wlan-sec-prof-huawei] wpa2 authentication-method dot1x peap
encryption-method tkip
```

- WPA2-802.1x+PEAP+CCMP，具体配置如下：

```
<Quidway> system-view
[Quidway] radius-server template radius_huawei
[Quidway-radius-radius_huawei] radius-server authentication 10.138.18.152 1812
[Quidway-radius-radius_huawei] radius-server accounting 10.138.18.152 1813
[Quidway-radius-radius_huawei] radius-server shared-key simple huawei
[Quidway-radius-radius_huawei] quit
[Quidway] aaa
[Quidway-aaa] authentication-scheme radius_huawei
[Quidway-aaa-authen-radius_huawei] authentication-mode radius
[Quidway-aaa-authen-radius_huawei] quit
[Quidway-aaa] accounting-scheme radius_huawei
[Quidway-aaa-accounting-radius_huawei] accounting-mode radius
[Quidway-aaa-accounting-radius_huawei] quit
[Quidway-aaa] domain peap.radius.com
[Quidway-aaa-domain-peap.radius.com] authentication-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] accounting-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] radius-server radius_huawei
[Quidway-aaa-domain-peap.radius.com] quit
[Quidway-aaa] quit
[Quidway] interface wlan-ess 0
[Quidway-Wlan-Ess0] dot1x-authentication enable
[Quidway-Wlan-Ess0] dot1x authentication-method eap
[Quidway-Wlan-Ess0] force-domain huawei
[Quidway-Wlan-Ess0] peimit-domain huawei
[Quidway-Wlan-Ess0] quit
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa2
[Quidway-wlan-sec-prof-huawei] wpa2 authentication-method dot1x peap
encryption-method ccmp
```

- WPA2-802.1x+TLS+TKIP，具体配置如下：

```
<Quidway> system-view
[Quidway] radius-server template radius_huawei
[Quidway-radius-radius_huawei] radius-server authentication 10.138.18.152 1812
[Quidway-radius-radius_huawei] radius-server accounting 10.138.18.152 1813
[Quidway-radius-radius_huawei] radius-server shared-key simple huawei
[Quidway-radius-radius_huawei] quit
[Quidway] aaa
[Quidway-aaa] authentication-scheme radius_huawei
[Quidway-aaa-authen-radius_huawei] authentication-mode radius
[Quidway-aaa-authen-radius_huawei] quit
[Quidway-aaa] accounting-scheme radius_huawei
[Quidway-aaa-accounting-radius_huawei] accounting-mode radius
[Quidway-aaa-accounting-radius_huawei] quit
[Quidway-aaa] domain peap.radius.com
[Quidway-aaa-domain-peap.radius.com] authentication-scheme radius_huawei
```

```
[Quidway-aaa-domain-peap.radius.com] accounting-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] radius-server radius_huawei
[Quidway-aaa-domain-peap.radius.com] quit
[Quidway-aaa] quit
[Quidway] interface wlan-ess 0
[Quidway-Wlan-Ess0] dot1x-authentication enable
[Quidway-Wlan-Ess0] dot1x authentication-method eap
[Quidway-Wlan-Ess0] force-domain huawei
[Quidway-Wlan-Ess0] peimit-domain huawei
[Quidway-Wlan-Ess0] quit
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa2
[Quidway-wlan-sec-prof-huawei] wpa2 authentication-method dot1x tls encryption-
method tkip
```

- WPA2-802.1x+TLS+CCMP，具体配置如下：

```
<Quidway> system-view
[Quidway] radius-server template radius_huawei
[Quidway-radius-radius_huawei] radius-server authentication 10.138.18.152 1812
[Quidway-radius-radius_huawei] radius-server accounting 10.138.18.152 1813
[Quidway-radius-radius_huawei] radius-server shared-key simple huawei
[Quidway-radius-radius_huawei] quit
[Quidway] aaa
[Quidway-aaa] authentication-scheme radius_huawei
[Quidway-aaa-authen-radius_huawei] authentication-mode radius
[Quidway-aaa-authen-radius_huawei] quit
[Quidway-aaa] accounting-scheme radius_huawei
[Quidway-aaa-accounting-radius_huawei] accounting-mode radius
[Quidway-aaa-accounting-radius_huawei] quit
[Quidway-aaa] domain peap.radius.com
[Quidway-aaa-domain-peap.radius.com] authentication-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] accounting-scheme radius_huawei
[Quidway-aaa-domain-peap.radius.com] radius-server radius_huawei
[Quidway-aaa-domain-peap.radius.com] quit
[Quidway-aaa] quit
[Quidway] interface wlan-ess 0
[Quidway-Wlan-Ess0] dot1x-authentication enable
[Quidway-Wlan-Ess0] dot1x authentication-method eap
[Quidway-Wlan-Ess0] force-domain huawei
[Quidway-Wlan-Ess0] peimit-domain huawei
[Quidway-Wlan-Ess0] quit
[Quidway] wlan
[Quidway-wlan-view] security-profile name huawei
[Quidway-wlan-sec-prof-huawei] security-policy wpa2
[Quidway-wlan-sec-prof-huawei] wpa2 authentication-method dot1x tls encryption-
method ccmp
```

## WAPI: SMS4 算法

中国颁布的 WLAN 规范定义了一种新的安全机制 WAPI，其认证框架采用基于证书的双向认证机制，支持 AP 与 STA 之间的双向鉴别。



WAPI 安全协议可匹配多种可用的密码算法，例如在中国使用 SMS4，在美国可以使用 AES，在韩国可以使用 SEED。

SMS4 算法已公开，请参考相关技术文档，本文不再赘述。

## 网络层加密协议

除了以上的加密方式，WLAN 还支持使用历经考验的网络层加密协议，例如 IPSec、SSL、SSH 等。

## 1.3 应用

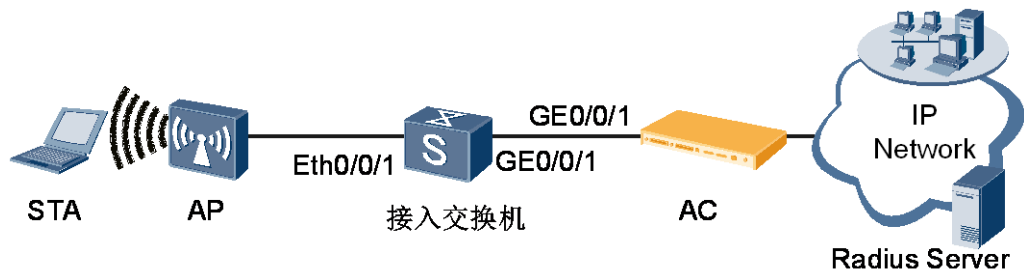
### 1.3.1 WPA+802.1X 认证示例

#### 组网需求

如图 1-17 所示，现有网络中 AC 连接上层网络中的 RADIUS 服务器，并通过接入交换机连接管理 AP。

若在无线网络中采取简单的安全策略，并不能完全保证无线网络的安全，无线网络中的加密数据还是存在被破解的风险。企业希望利用 RADIUS 服务器在无线网络中配置 802.1X 认证，完全保证无线网络安全。

图1-17 配置 WPA+802.1X 认证组网图



#### 配置思路

采用如下的思路在 Router 上进行配置：

配置 802.1X 认证。

1. 在系统视图下开启全局 802.1X 认证。
2. 配置 802.1X 认证时使用的 RADIUS 方案。
3. 创建 802.1X 认证时使用的域，并在域中引用 RADIUS 方案作为 AAA 的认证方案。

配置 AC：

1. 配置 Switch 和 AC，实现 AP 和 AC 互通。

2. 配置 AC 的基本功能，包括配置 AC 运营商标识和 ID、AC 与 AP 之间通信的源接口，实现 AC 作为 DHCP Server 功能。
3. 配置 AP 上线的认证方式，并把 AP 加入 AP 域中，实现 AP 正常工作。
4. 配置 VAP，下发 WLAN 业务，实现 STA 访问 WLAN 网络功能。

其中配置 VAP，需要：

- a. 配置 WLAN-ESS 接口，并在服务集下绑定该接口，实现无线侧报文到达 AC 后能够送至 WLAN 业务处理模块功能。
- b. 配置 AP 对应的射频模板，并在射频下绑定该模板，实现 STA 与 AP 之间的无线通信参数配置。
- c. 配置 AP 对应的安全模板，配置安全策略为 WPA+802.1X+PEAP+CCMP。
- d. 配置 AP 对应的服务集，并在服务集下配置数据直接转发模式，绑定安全模板、流量模板，实现 STA 接入网络安全策略及 QoS 控制。
- e. 配置 VAP 并下发，实现 STA 访问 WLAN 网络功能。

## 配置文件

- AC 的配置文件

```
#
sysname AC
#
vlan batch 101 800
#
dhcp enable
#
wlan ac-global carrier id other ac id 1
#
radius-server template radius_huawei
radius-server authentication 10.1.1.5 1812
radius-server accounting 10.1.1.5 1813
#
aaa
authentication-scheme radius_huawei
authentication-mode radius
accounting-scheme radius_huawei
accounting-mode radius
domain peap.radius.com
authentication-scheme radius_huawei
accounting-scheme radius_huawei
radius-server radius_huawei
#
interface Vlanif101
ip address 128.1.1.1 255.255.255.0
dhcp select interface
#
interface Vlanif800
ip address 172.1.1.1 255.255.255.0
dhcp select interface
#
interface WLAN-ESS0
port hybrid pvid vlan 101
port hybrid untagged vlan 101
```

```
dot1x-authentication enable
dot1x authentication-method eap
permit-domain peap.domain.com
force-domain peap.domain.com
#
interface XGigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 101 800
#
wlan
wlan ac source interface vlanif800
ap-region id 101
ap-auth-mode mac-auth
ap id 1 type-id 6 mac 286E-D42B-0CE5 sn AB34002078
region-id 101
wmm-profile name huawei-ap id 0
traffic-profile name huawei-ap id 0
security-profile name huawei-ap id 0
security-policy wpa
wpa authentication-method dot1x peap encryption-method ccmp
service-set name huawei id 0
wlan-ess 0
ssid huawei
traffic-profile id 0
security-profile id 0
service-vlan 101
radio-profile name huawei-ap id 0
wmm-profile id 0
ap 1 radio 0
radio-profile id 0
service-set id 0 wlan 1
#
return
```

## 1.3.2 Portal 认证

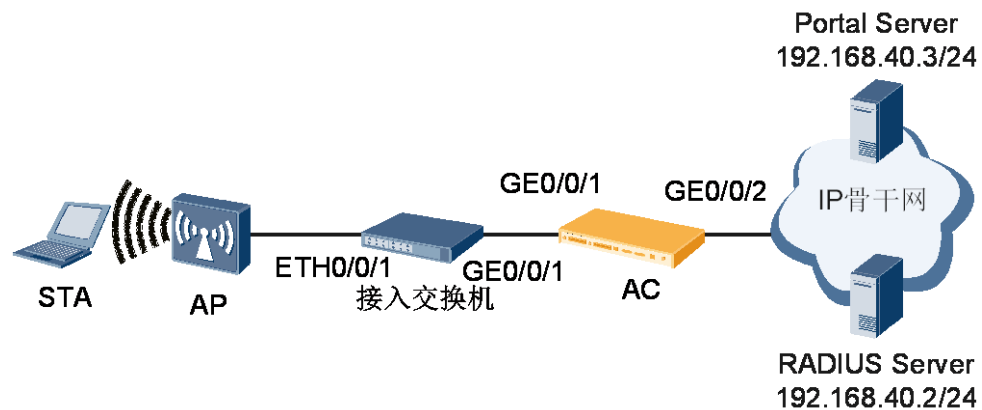
### 组网需求

如图 1-18 所示，现有网络中 AC 连接 Portal 服务器和 RADIUS 服务器，并通过接入交换机连接管理 AP。

由于无线网络开放性的特点，若无线网络不采取适当的安全策略，用户数据就存在安全风险。管理员要求如下：

- 用户通过 AC 完成 Portal 认证。
- 使用 RADIUS 完成认证和计费。
- 用户在未通过 Portal 认证前，只能访问 Portal 服务器。
- 用户通过 Portal 认证后，可以正常访问外部网络。

图1-18 配置无线 Portal 认证组网图



采用如下的思路在 AC 上配置。

1. 配置接入交换机、AC 有线侧和无线侧接口，保证各个设备之间网络互通。
2. 配置 Portal 认证时使用的 RADIUS 方案。
3. 创建 Portal 认证时使用的域，并在域中引用 RADIUS 方案作为 AAA 的认证方案。
4. 配置 Portal 服务器，并在用户 VLAN 下进行绑定。
5. 在 AC 上配置 WLAN 相关业务。
6. 业务下发至 AP，用户完成业务验证。

## 配置文件

- AC 的配置文件

```
#
sysname AC
#
vlan batch 101 800
#
dhcp enable
#
radius-server template radius_huawei
radius-server authentication 192.168.40.2 1812
radius-server accounting 192.168.40.2 1813
#
web-auth-server test
server-ip 192.168.40.3
port 50100
shared-key simple huawei
url http://192.168.40.3
#
aaa
authentication-scheme radius_huawei
authentication-mode radius
accounting-scheme radius_huawei
accounting-mode radius
```

```
domain peap.radius.com
authentication-scheme radius_huawei
accounting-scheme radius_huawei
radius-server radius_huawei
#
wlan ac-global carrier id other ac id 1
#
interface Vlanif101
ip address 192.168.20.1 255.255.255.0
dhcp select interface
web-auth-server test direct
#
interface Vlanif200
ip address 192.168.40.1 255.255.255.0
web-auth-server test direct
#
interface Vlanif800
ip address 192.168.10.1 255.255.255.0
dhcp select interface
#
interface WLAN-ESS0
port hybrid untagged vlan 101
mac-authentication enable
permit-domain radius_huawei
force-domain radius_huawei
dhcp enable
#
interface XGigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 101 200 800
#
interface GigabitEthernet0/0/2
port link-type access
port default vlan 200
#
wlan
wlan ac source interface vlanif800
ap-region id 101
ap-auth-mode mac-auth
ap id 1 type-id 6 mac 286E-D42B-0CE5 sn AB34002078
region-id 101
wmm-profile name huawei id 0
traffic-profile name huawei id 0
security-profile name huawei id 0
wep authentication-method share-key
wep key wep-40 pass-phrase 0 simple 12345
service-set name huawei id 0
wlan-ess 0
ssid huawei-portal-test
traffic-profile id 0
security-profile id 0
service-vlan 101
radio-profile name huawei-ap id 0
wmm-profile id 0
ap 1 radio 0
```

```
radio-profile id 0
service-set id 0 wlan 1
#
return
```