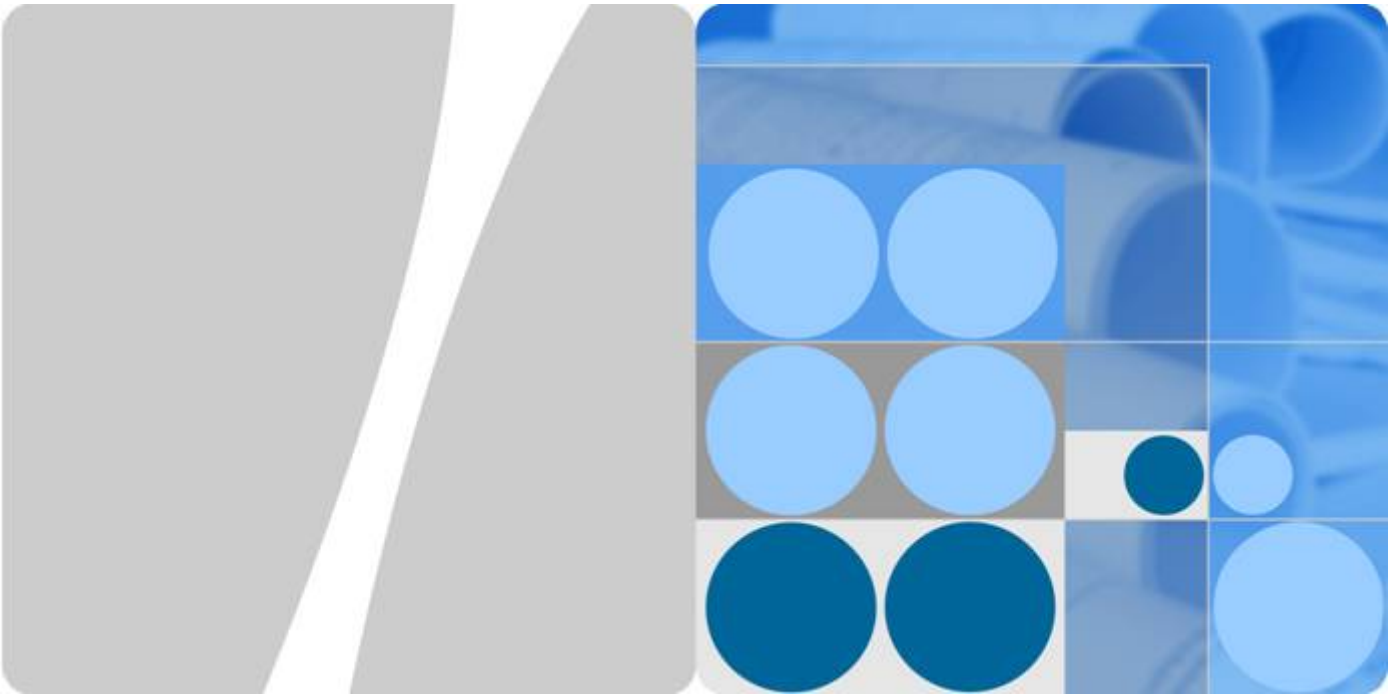


Huawei AR1200 系列企业路由器

V200R002C00

特性描述-WLAN

文档版本　01

发布日期　2011-12-30

华为技术有限公司

商标声明


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://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前 言

读者对象

本文档针对可靠性特性，从简介、原理描述和应用三个方面介绍了 WLAN 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	以本标志开始的文本表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
警告	以本标志开始的文本表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。
说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

命令行格式约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... }*	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...]*	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复 1 ～ n 次。
#	由“#”开始的行表示为注释行。

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 01 (2011-12-30)

第一次正式发布。

目 录

1 WLAN 特性描述

关于本章

1.1 介绍

定义

WLAN 全称是 Wireless Local Area Network，即无线局域网，指应用无线通信技术将计算机设备互联起来，构成可以互相通信和实现资源共享的网络体系。它是一种利用无线技术实现快速接入以太网的技术。无线局域网本质的特点是不再使用通信电缆将计算机与网络连接起来，而是通过无线的方式连接，从而使网络的构建和终端的移动更加灵活。和传统的有线接入方式相比，无线局域网让网络使用更自由。

无线局域网使用无线电波作为数据传送的媒介，传送距离一般为几十米。无线局域网的主干网络通常使用电缆（Cable），无线局域网用户通过一个或更多无线接取器 AP（Access points）接入无线局域网。无线局域网现在已经广泛的应用在商务区、大学、机场及其他公共区域。

无线局域网最通用的标准是 IEEE 定义的 802.11 系列标准。

目的

WLAN（Wireless Local Area Network，无线局域网)技术是当今通信领域的热点之一，和有线相比，无线局域网的启动和实施相对简单，成本相对低廉，一般只要安放一个或多个接入点设备就可建立覆盖整个建筑或地区的局域网络。然而，WLAN 系统不是完全的无线系统，它的服务器和骨干网仍然安置在固定网络，只是用户可以通过无线方式接入网络。

WLAN 最大的优势就是免去或减少了繁杂的网络布线，另外对于地铁、公路交通监控等难于布线的场所，无线局域网的应用越来越广泛。

受益

- 用户受益

  WLAN 接入作为传统接入方式的补充，可以覆盖家庭、宾馆、写字楼、酒店大堂、车站、机场等热点区域，提供移动服务，使得固定网络接入延伸到了家庭以外的地方。
- 企业受益

  使用 WLAN 解决方案，企业能够为用户提供方便的无线接入服务，主要包括：
  - 通过无线网络，用户可以方便的接入到无线网络，并访问已有网络或因特网；
  - 安全问题是无线网络最大的挑战，当前无线网络可以使用不同认证和加密方式，提供安全的无线网络接入服务；
  - 在无线网络内，无线用户可以在网络覆盖区域内自由移动，彻底摆脱有线束缚。

1.2 参考标准和协议

表 1-1 参考标准和协议

文档	描述
RFC 5416	Control and Provisioning of Wireless Access Points Protocol Binding for IEEE 802.11
IEEE 802.11	无线网络通信的标准
IEEE 802.1X	基于端口的链路认证
IEEE 802.11e	对服务等级（Quality of Service, QoS）的支持
RFC 5415	Control And Provisioning of Wireless Access Points Protocol Specification

1.3 可获得性

涉及网元

表 1-2 WLAN 特性涉及到的网元

网元	描述
无线接入点 AP	完成无线终端数据到有线数据的转换和接入功能。
RADIUS 服务器	完成 WLAN 用户 RADIUS 认证、授权、计费功能。
企业网管	实现无线控制器的企业网管功能。

License 支持

无。

版本支持

表 1-3 支持的版本

产品	支持版本
AR1200	V200R001C00

特性依赖

WLAN 特性与其他特性的依赖关系如下:

- WLAN 特性的 AAA 功能需要依赖 AAA 特性。
- WLAN 特性的 L3 转发功能依赖 IPv4 路由和协议栈。
- WLAN 特性的 L2 转发功能依赖二层转发特性。
- WLAN 特性的接入和安全功能依赖 DOT1X 特性。

硬件要求

目前支持 WLAN 特性的 AR 型号：AR1220W、AR1220VW、AR1220W-S。

系统性能

表 1-4 系统性能表

规格项	规格数
AP 允许接入的最大用户数	128
支持的 WMM 模板	16
支持的安全模板	16

1.4 原理描述

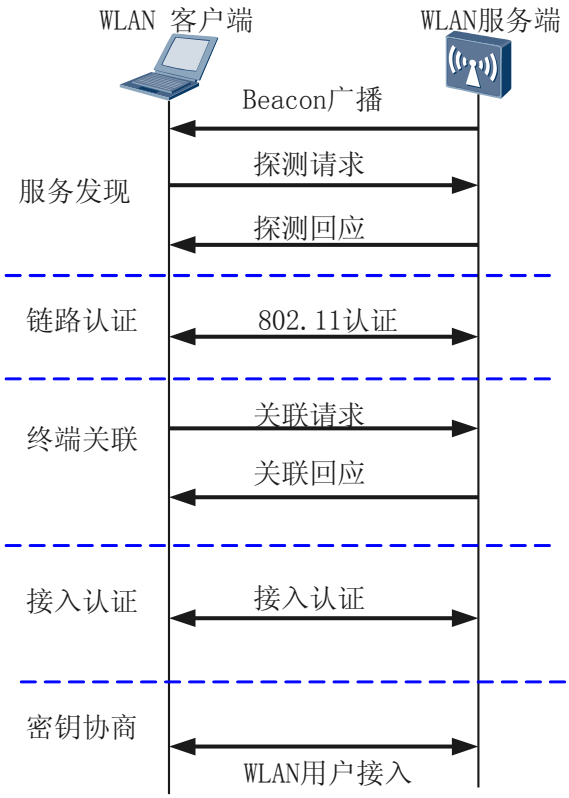
1.4.1 WLAN 用户接入

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。

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



如图 1-1 所示，步骤说明如下：

1. WLAN 服务发现

   WLAN 客户端有两种方式可以发现 WLAN 服务，目前 AR1200 的 WLAN 同时支持这两种方式：

   - 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

   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。

   其中开放认证其实是不认证、不加密，只要 WLAN 服务端支持该认证方式，WLAN 客户端就可以链路认证成功。

   Shared Key 认证是指客户端和服务端配置相同的共享密钥，WLAN 服务端在链路认证过程验证两边的密钥配置是否相同，如果一致，则认证成功，否则认证失败。

   链路认证的详细介绍请参见 **1.4.2 802.11 链路认证**。

说明

802.11 定义了一套链路协商机制，其中包括 802.11 链路认证过程和 802.11 链接协商过程。只有当 WLAN 客户端成功发现 WLAN 服务，并且和 WLAN 服务端成功完成链路认证和链接协商后，客户端和服务端才成功的建立 802.11 链路，客户端才能访问网络。

3. 终端关联

终端关联过程实质上是链路服务协商的过程。完成了 802.11 的链路认证后，WLAN 客户端会继续发起 802.11 链路服务协商，具体的协商通过 Association 报文或者 Re-association 报文实现。

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。AR1200 接入认证主要有 **1.4.9 802.1X 认证**、**1.4.8 MAC 认证**、**1.4.7 PSK 认证**。其中 802.1x 接入认证、MAC 接入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 **1.4.6 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。

说明

通常 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。

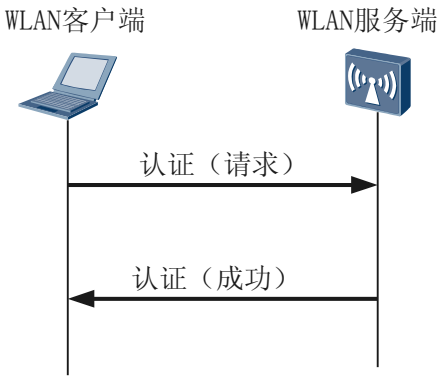
1.4.2 802.11 链路认证

WEP（Wired Equivalent Privacy）开放认证

WEP 开放认证是最简单的 802.11 链路认证算法，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：第一

步是客户端发起认证请求，第二步 WLAN 服务端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。如图 1-2 所示。

图 1-2 WEP 开放认证



WLAN用户接入

WEP 开放认证其实没有对用户进行任何认证操作，只是根据 WLAN 服务是否支持开放认证确定对客户端的认证是否成功，也不会对客户端的无线报文进行加密。当 WLAN 提供 RSN 以及 WPA 的安全服务时，链路认证必须使用开放认证，而不能使用 Shared Key 认证。

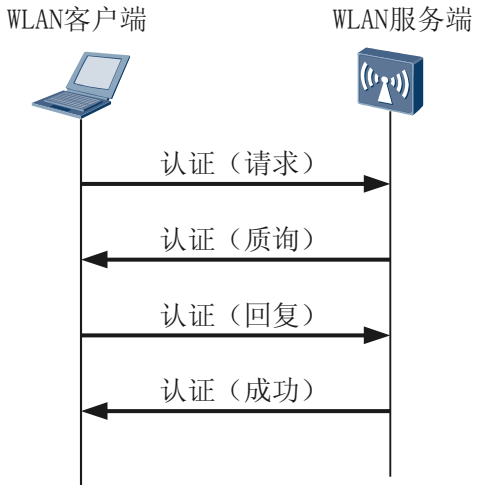
虽然 IEEE802.11-1999 协议已经考虑到了无线局域网的安全问题，并且定义了相应的安全机制以及 WEP 加密机制（基于 RC4 对称流加密算法，而且需要预先配置相同的静态 Key）；但是无论从加密机制还是加密算法本身，WEP 加密机制都容易受到安全威胁。随着无线局域网的发展，IEEE802.11i 比较彻底的解决无线局域网的安全问题（特别采用了更加高级的加密算法 AES，通过密钥协商实现动态密钥管理和更新，结合了 802.1x 接入认证为无线局域网提供安全保护）。

在 IEEE802.11 标准的新安全方案确定前，WEP 是唯一的选择，虽然目前已经证明这种认证方式极不安全，但是有时候某些特殊设备，只支持 WEP，而且 WEP 的设计也很容易实现，也没有后续出现的加密协议复杂，不要求多么强的处理能力，很适合安全性要求不高的应用场景，例如某些手持终端，软件和硬件的处理能力比较弱。

WEP 共享密钥认证

WEP 共享密钥认证是另外一种 802.11 链路认证机制。共享密钥认证需要 WLAN 客户端和 WLAN 服务端配置相同的共享密钥。

图 1-3 WEP Sharekey 认证



如图 1-3 所示，共享密钥认证的认证过程为：

1. WLAN 客户端先向 WLAN 服务端发送认证请求。
2. WLAN 服务端会随机产生一个 Challenge 字符串发送给客户端。
3. WLAN 客户端会将接收到字符串拷贝到新的消息中，用密钥加密后再发送给服务端。
4. WLAN 服务端接收到该消息后，用密钥将该消息解密，然后对解密后的字符串和最初给客户端的字符串进行比较。如果相同，则说明客户端拥有服务端相同的共享密钥，即通过了 Shared Key 认证；否则 Shared Key 认证失败。

说明

- WEP 共享密钥认证采用的 WEP 加密机制是基于 RC4 对称流加密算法，而且需要预先配置相同的静态 Key，但是无论从加密机制还是加密算法本身，WEP 加密机制都容易受到安全威胁。
- WEP 共享密钥认证安全性比 WEP 开放认证的安全性略高，但它本质上是一种静态密钥认证方式，并不能从根本上解决无线安全问题。
- 对于小型企业和家庭用户而言，无线接入用户数量比较少，一般没有专业的 IT 管理人员，对网络安全性的要求相对较低。通常情况下不会配备专用的认证服务器，这种情况下，可直接采用 WEP 进行认证，WEP-ShareKey+接入点隐藏可以保证基本的安全级别。

1.4.3 WEP 服务

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。

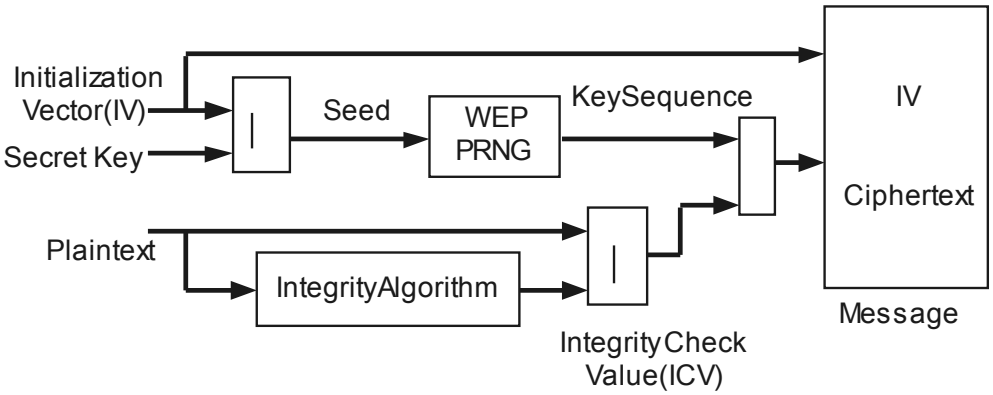
WEP 认证

以 WEP 共享密钥认证为例，认证过程请参考 **1.4.2 802.11 链路认证**的“WEP 共享密钥认证流程”。

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。

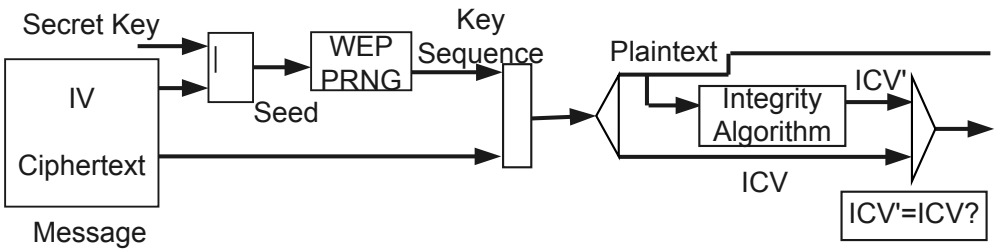
图 1-4 WEP 加密原理图



如**图 1-4** 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 1-5 WEP 解密原理图



如**图 1-5** 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。

有线对等保密 WEP 协议是 IEEE802.11 标准中提出的认证加密方法。它使用 RC4 流密码来保证数据的保密性，通过共享密钥来实现认证，理论上增加了网络侦听，会话截获等的攻击难度。由于其使用固定的加密密钥和过短的初始向量，加上无线局域网的通信速度非常高，该方法已被证实存在严重的安全漏洞，在 15 分钟内就可被攻破。现在已有专门的自由攻击软件（如 airsnort）。而且这些安全漏洞和 WEP 对加密算法的使用机制有关，即使增加密钥长度也不可能增加安全性。另外，WEP 缺少密钥管理。用户的加密密钥必须与 WLAN 服务端的密钥相同，并且一个服务区内的所有用户都共享同一把密钥。WEP 中没有规定共享密钥的管理方案，通常是手工进行配置与维护。由于同时更换密钥的费时与困难，所以密钥通常很少更换，倘若一个用户丢失密钥，则会殃及到整个网络的安全。

WEP ICV 是一种基于 CRC-32 的用于检测传输噪音和普通错误的算法。CRC-32 是信息的线性函数，这意味着攻击者可以篡改加密信息，并很容易地修改 ICV。

1.4.4 WPA 服务

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 的替换品，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 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-Dot.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：对一些中小型的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(WLAN 服务端、无线路由器、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，而不用于加密过程，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

  WPA 与 WEP 相比，WEP 使用一个静态的密钥来加密所有的通信。而 WPA 不断的转换密钥。WPA 采用有效的密钥分发机制，可以跨越不同厂商的无线网卡实现应用。另外 WPA 的另一个优势是，它使公共场所和学术环境安全地部署无线网络成为可能。而在此之前，这些场所一直不能使用 WEP。WEP 的缺陷在于其加密密钥为静态密钥而非动态密钥。这意味着，为了更新密钥，IT 人员必须亲自访问每台机器，而这在学术环境和公共场所是不可能的。另一种办法是让密钥保持不变，而这会使用户容易受到攻击。由于互操作问题，学术环境和公共场所一直不能使用专有的安全机制。

- 数据加密

  WPA 支持的加密算法有两种：TKIP 和 CCMP。

  - TKIP

    WPA 采用 TKIP 为加密引入了新的机制，它使用一种密钥构架和管理方法，通过由认证服务器动态生成分发的密钥来取代单个静态密钥、把密钥首部长度从 24 位增加到 48 位等方法增强安全性。而且，TKIP 利用了 802.1x/EAP 服务端构架。认证服务器在接受了用户身份后，使用 802.1x 产生一个唯一的主密钥处理会话。然后，TKIP 把这个密钥通过安全通道分发到 WLAN 服务端和客户端，并建立起一个密钥构架和管理系统，使用主密钥为用户会话动态产生一个唯一的数据加密密钥，来加密每一个无线通信数据报文。TKIP 的密钥构架使 WEP 静态单一的密钥变成了 500 万亿可用密钥。虽然 WPA 采用的还是和 WEP 一样的 RC4 加密算法，但其动态密钥的特性很难被攻破。

    TKIP 与 WEP 一样基于 RC4 加密算法，但相比 WEP 算法，TKIP 密钥的长度由 40 位加长到 128 位，初始化向量 IV 的长度由 24 位加长到 48 位，并对现有的 WEP 进行了改进，即追加了“每发一个包重新生成一个新的密钥(Per Packet Key)”、“消息完整性检查（MIC）”、“具有序列功能的初始向量”和“密钥生成和定期更新功能”四种算法，极大地提高了加密安全强度。

    TKIP 只能作为一种临时的过渡方案，而 IEEE802.11i 标准的最终方案是基于 IEEE802.1x 认证的 CCMP（CBC-MAC Protocol）加密技术，即以 AES（Advanced Encryption Standard）为核心算法。它采用 CBC-MAC 加密模式，具有分组序号的初始向量。CCMP 为 128 位的分组加密算法，相比前面所述的所有算法安全程度更高。

  - 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 Autentication Code）。CCM 保护 MPDU 数据和 IEEE802.11 MPDU 帧头部分域的完整性。

- 完整性校验（MIC）

  为了防止攻击者从中间截获数据报文、篡改后重发而设置的。除了和 802.11 一样继续保留对每个数据分段(MPDU)进行 CRC 校验外，WPA 为 802.11 的每个数据分组

(MSDU)都增加了一个 8 个字节的消息完整性校验值，这和 802.11 对每个数据分段(MPDU)进行 ICV 校验的目的不同。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。而 WPA 中的 MIC 则是为了防止黑客的篡改而定制的，它采用 Michael 算法，具有很高的安全特性。当 MIC 发生错误的时候，数据很可能已经被篡改，系统很可能正在受到攻击。此时，WPA 还会采取一系列的对策，比如立刻更换组密钥等，来阻止黑客的攻击。

WPA 和 WEP 主要区别：

1. WEP 采用静态密钥，WPA 采用密钥协商机制，使用动态密钥，用户每次上线都协商出不同密钥。
2. WEP 采用的数据加密算法为 RC4 算法，WPA 采用 TKIP/CCMP。
3. WEP 采用 Open 和 ShareKey 认证，WPA 采用 WPA-PSK 和 WPA-DOT1X 认证。

1.4.5 WAPI 服务

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。

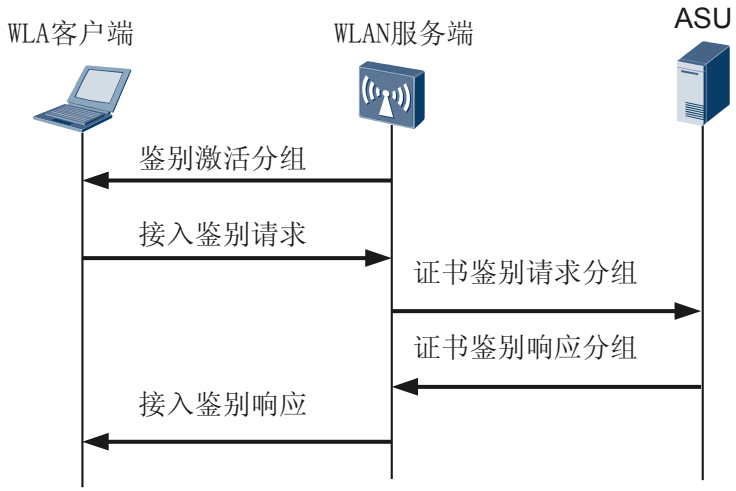
WAPI-PSK： 若采用预共享密钥的方式，整个过程则为单播密钥协商与组播密钥通告。预共享密钥鉴别是基于 WLAN 客户端与 WLAN 服务端双方的预共享密钥所进行的鉴别。鉴别前 WLAN 客户端与 WLAN 服务端必须预先配置有相同的密钥，即预共享密钥。鉴别时直接将预共享密钥转换为 BK（基密钥），然后进行单播密钥协商和组播密钥通告。在单播密钥协商和组播密钥通告成功之后，WLAN 客户端与 WLAN 服务端才可以开始数据传输，数据传输时使用协商出来的密钥对它们之间的数据进行加解密，加密算法采用 WPISMS4

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 1-6 WAPI 证书鉴别



如图 1-6 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。

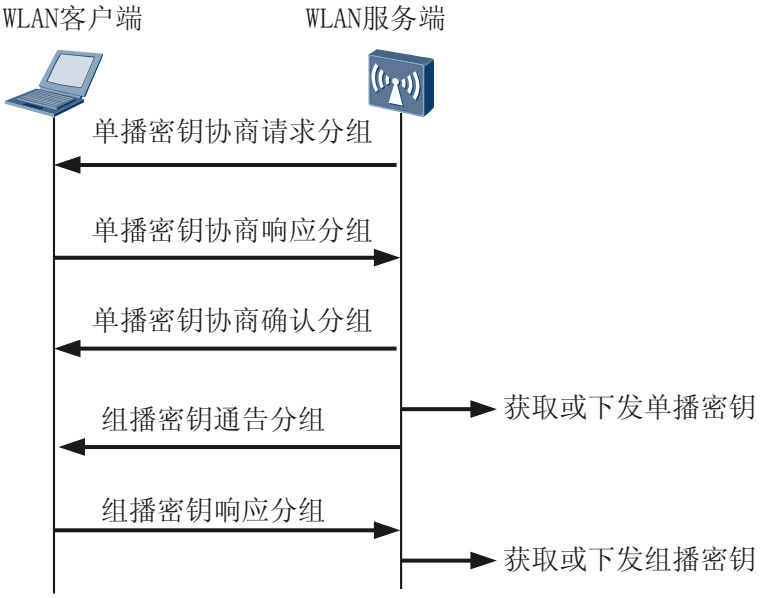
- WAPI 密钥协商

  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 1-7 WAPI 密钥协商



如图 1-7 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：

1. 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。
2. 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。
3. 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。

1.4.6 EAPOL-Key 密钥协商

WPA 的四次握手在主密钥 PMK 生成之后，不管是采用 802.1X 认证还是预共享密钥认证方式，都会有四次握手过程的产生，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。

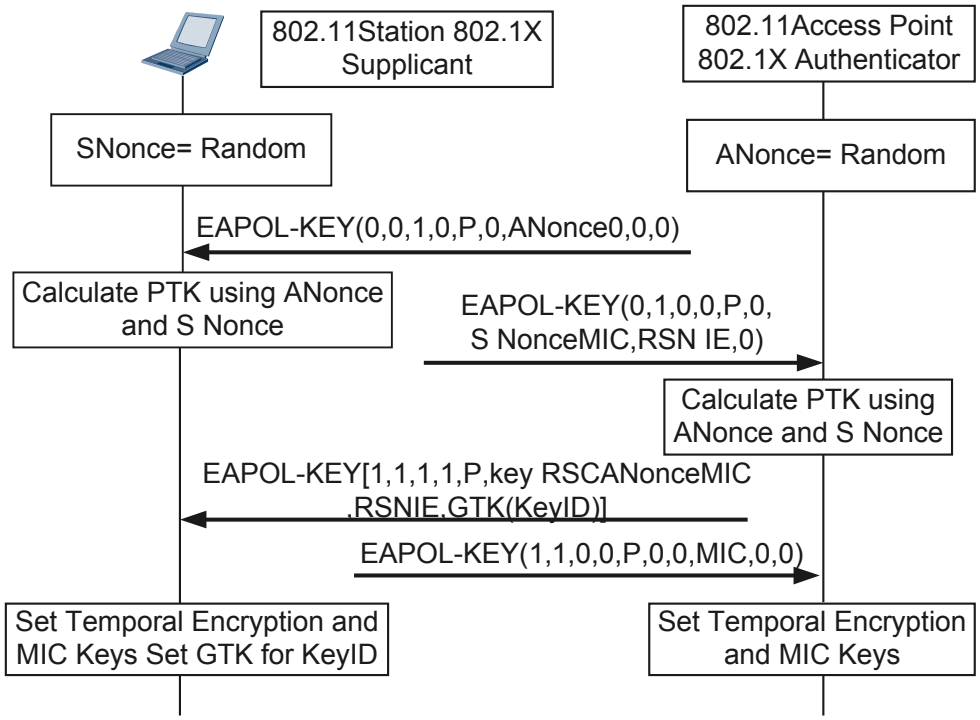
在 802.l1i 里定义了两种密钥层次模型，一种是成对密钥层次结构，主要用来描述一对设备之间的所有密钥；一种是组密钥层次结构，主要用来描述全部设备所共享的各种密钥。

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 1-8 EAPOL-Key 单播密钥协商



如图 1-8 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)。
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 服务端的 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。

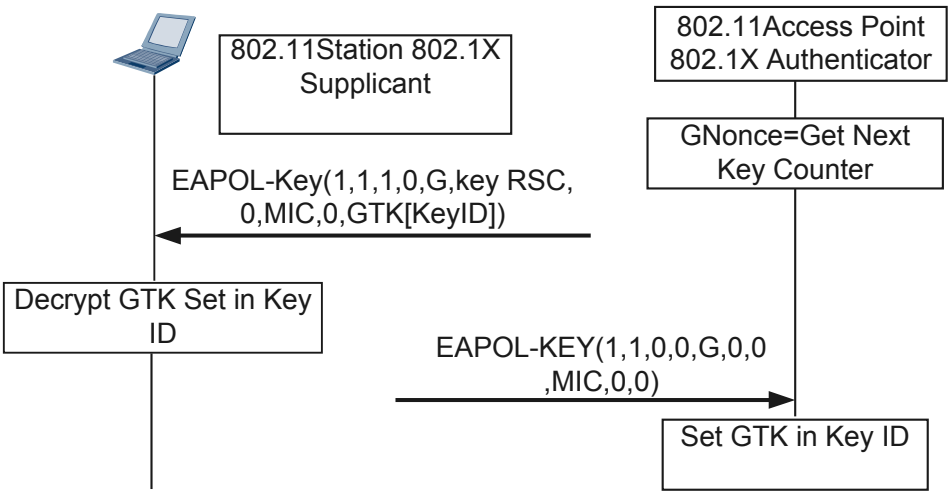
- 二次组播密钥协商过程

  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 1-9 EAPOL-Key 多播密钥协商



如图 1-9 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。

1.4.7 PSK 认证

PSK 认证需要实现在客户端和服务端配置相同的预共享密钥，而具体的认证过程实际上在密钥协商过程（EAPOL-Key 密钥协商过程）中完成。在密钥协商过程中，预共享密钥将作为输入之一生成密钥协商使用的 PMK。

可以通过是否能够对协商的消息成功解密，来确定本端配置的预共享密钥是否和对端配置的预共享密钥相同，完成服务端和客户端的互相认证。如果密钥协商成功，则表明 PSK 接入认证成功；如果密钥协商失败，则可以认为 PSK 接入认证失败。

PSK 认证用于 WPA/WPA2 服务时，WPA/WPA2 预共享密钥作为生成 PMK 的输入之一，然后基于 PMK，进行 EAPOL-Key 密钥协商过程，根据密钥协商结果确定 PSK 认证结果，PSK 认证过程即密钥协商过程请参考 **1.4.6 EAPOL-Key 密钥协商**章节。

PSK 认证用于 WAPI 服务时，WAPI 预共享密钥作为转换 BK 的输入，然后基于 BK，进行 WAPI 密钥协商过程，根据密钥协商结果确定 PSK 认证结果，PSK 认证过程即密钥协商过程请参考 **1.4.5 WAPI 服务**章节的“WAPI 密钥协商”。

1.4.8 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。

1.4.9 802.1X 认证

IEEE802 LAN/WAN 委员会为解决无线局域网网络安全问题，提出了 802.1X 协议。后来，802.1X 协议作为局域网端口的一个普通接入控制机制在以太网中被广泛应用，主要解决以太网内认证和安全方面的问题。在 WLAN 中，802.1X 通常和 WPA 服务和 EAPOL-Key 密钥协商结合使用。

802.1X 协议是一种基于端口的网络接入控制协议（port based network access control protocol）。“基于端口的网络接入控制”是指在局域网接入设备的端口这一级对所接入的用户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。

802.1X 认证系统使用 EAP（Extensible Authentication Protocol）来实现客户端、服务端和认证服务器之间认证信息的交换。

在客户端与服务端之间，EAP 协议报文使用 EAPOL 封装格式，直接承载于 LAN 环境中。在服务端与 RADIUS 服务器之间，可以使用两种方式来交换信息。一种是 EAP 协议报文，由服务端进行中继，使用 EAPOR（EAP over RADIUS）封装格式承载于 RADIUS 协议中；另一种是 EAP 协议报文，由服务端进行终结，采用包含 PAP（Password Authentication Protocol）或 CHAP（Challenge Handshake Authentication Protocal）属性的报文与 RADIUS 服务器进行认证交互。

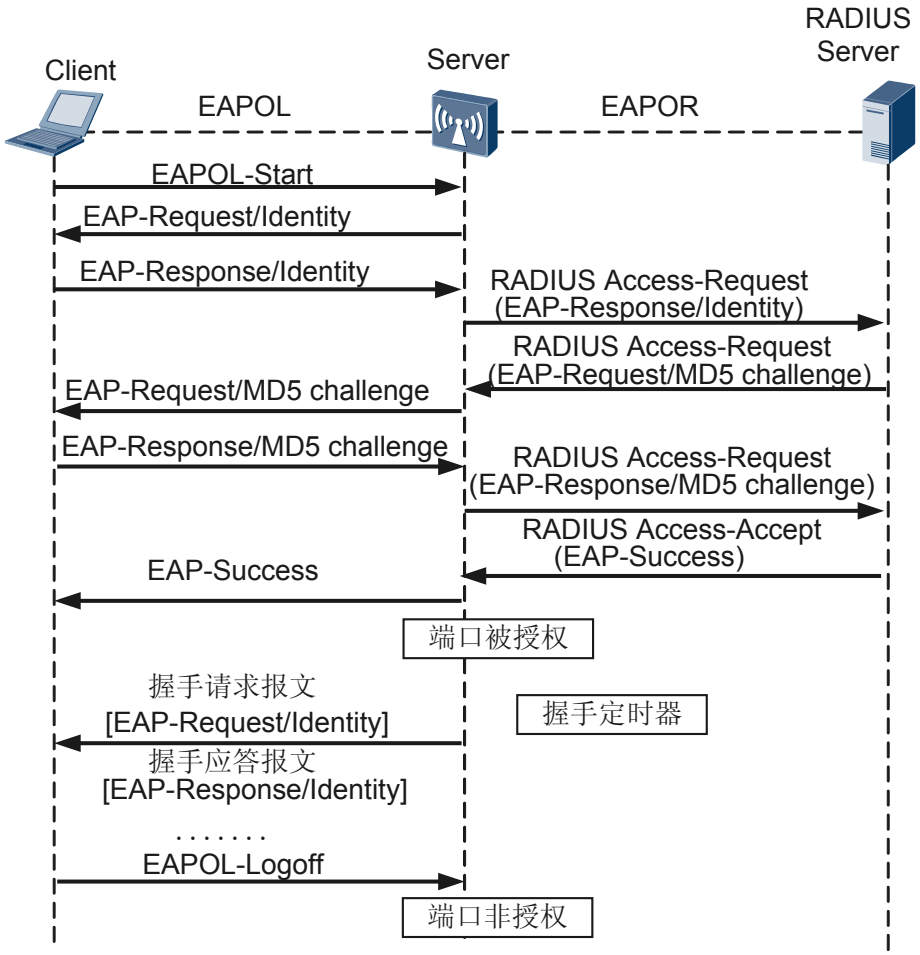
802.1X 系统支持 EAP 中继方式和 EAP 终结方式与远端 RADIUS 服务器交互完成认证。以下关于两种认证方式的过程描述，都以客户端主动发起认证为例。

- EAP 中继方式

  这种方式是 IEEE 802.1X 标准规定的，将 EAP 承载在其它高层协议中，如 EAP over RADIUS，以便扩展认证协议报文穿越复杂的网络到达认证服务器。一般来说，EAP 中继方式需要 RADIUS 服务器支持 EAP 属性：EAP-Message 和 Message-Authenticator，分别用来封装 EAP 报文及对携带 EAP-Message 的 RADIUS 报文进行保护。

  EAP 中继方式下，需要保证在 WLAN 客户端、WLAN 服务端和 RADIUS 服务器上选择一致的 EAP 认证方法，下面以 EAP-MD5 方式为例介绍基本业务流程。

图 1-10 EAP 中继认证



如图 1-10 所示，认证过程如下：

1. 当用户有访问网络需求时打开 802.1X 客户端程序，输入已经申请、登记过的用户名和密码，发起连接请求（EAPOL-Start 报文）。此时，客户端程序将发出请求认证的报文给服务端，开始启动一次认证过程。
2. 服务端收到请求认证的数据帧后，将发出一个请求帧（EAP-Request/Identity 报文）要求用户的客户端程序发送输入的用户名。
3. 客户端程序响应服务端发出的请求，将用户名信息通过数据帧（EAP-Response/Identity 报文）发送给服务端。服务端将客户端发送的数据帧经过封包处理后（RADIUS Access-Request 报文）送给认证服务器进行处理。
4. RADIUS 服务器收到服务端转发的用户名信息后，将该信息与数据库中的用户名表对比，找到该用户名对应的密码信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字通过 RADIUS Access-Challenge 报文发送给服务端，由服务端转发给客户端程序。
5. 客户端程序收到由服务端传来的加密字（EAP-Request/MD5 Challenge 报文）后，用该加密字对密码部分进行加密处理（此种加密算法通常是不可逆的），生成 EAP-Response/MD5Challenge 报文，并通过服务端传给 RADIUS 服务器。
6. RADIUS 服务器将收到的已加密的密码信息（RADIUS Access-Request 报文）和本地经过加密运算后的密码信息进行对比，如果相同，则认为该用户为合法

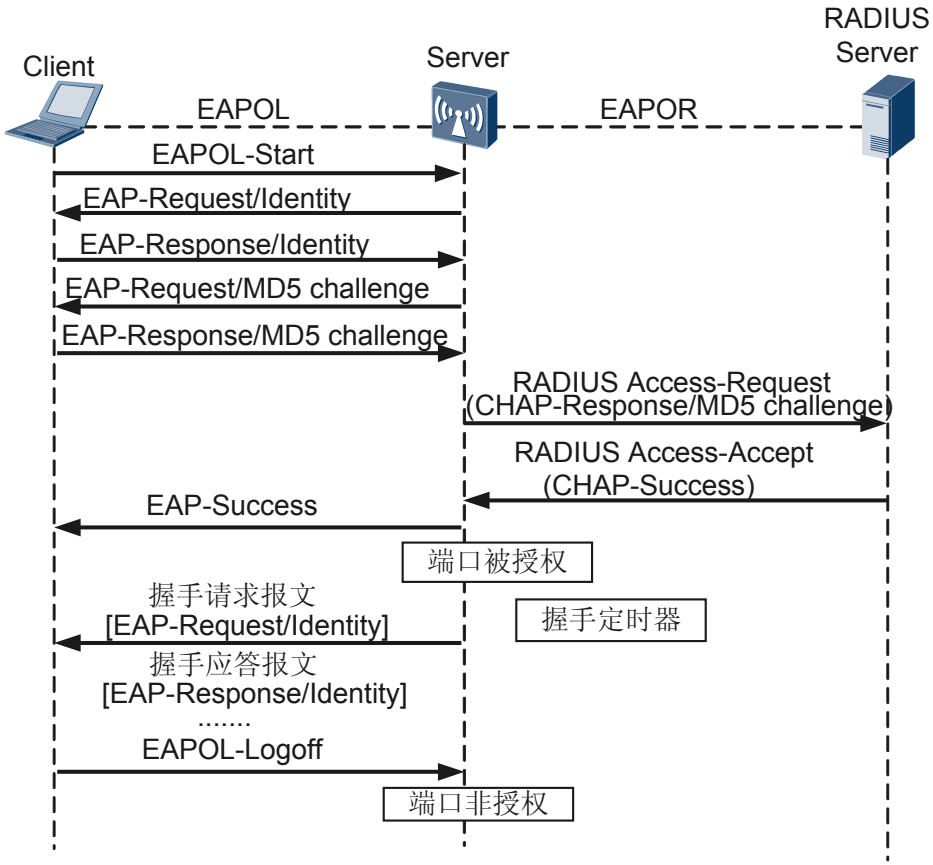
用户，反馈认证通过的消息（RADIUS Access-Accept 报文和 EAP-Success 报文）。

7. 服务端收到认证通过消息将端口改为授权状态，允许用户通过端口访问网络。在此期间，服务端会通过向客户端定期发送握手报文的方法，对用户的在线情况进行监测。缺省情况下，两次握手请求报文都得不到客户端应答，服务端就会让用户下线，防止用户因为异常原因下线而服务端无法感知。
8. 客户端也可以发送 EAPOL-Logoff 报文给服务端，主动要求下线。服务端把端口状态从授权状态改变成未授权状态，并向客户端发送 EAP-Failure 报文。

- EAP 终结方式

  这种方式将 EAP 报文在服务端终结并映射到 RADIUS 报文中，利用标准 RADIUS 协议完成认证、授权和计费。服务端与 RADIUS 服务器之间可以采用 PAP 或者 CHAP 认证方法。以下以 CHAP 认证方法为例介绍基本业务流程。如图 1-11 所示。

  图 1-11 EAP 终结认证



EAP 终结方式与 EAP 中继方式的认证流程相比，不同之处在于用来对用户密码信息进行加密处理的随机加密字由服务端生成，之后服务端会把用户名、随机加密字和客户端加密后的密码信息一起送给 RADIUS 服务器，进行相关的认证处理。

1.4.10 WLAN 安全

WLAN 具有安装便捷、使用灵活、经济节约、易于扩展等有线网络无法比拟的优点，因此 WLAN 得到越来越广泛的使用。但是由于 WLAN 信道开放的特点，使得攻击者能够很容易的进行窃听，恶意修改并转发，因此安全性成为阻碍其发展的最重要因素。

就目前而言，有很多种 WLAN 的安全技术，包括物理地址（MAC）过滤、服务区标识符(SSID)匹配、有线对等保密（WEP）、端口访问控制技术（IEEE802.1x）、WPA(Wi-Fi Protected Access)、IEEE 802.11i 等。

- WLAN 面临的安全威胁

  利用 WLAN 进行通信必须具有较高的通信保密能力。对于现有的 WLAN 产品，它的安全隐患主要有以下几点：

  - 未经授权使用网络服务

    由于 WLAN 的开放式访问方式，非法用户可以未经授权而擅自使用网络资源，不仅会占用宝贵的无线信道资源，增加带宽费用，降低合法用户的服务质量，而且未经授权的用户没有遵守运营商提出的服务条款，甚至可能导致法律纠纷。

  - 地址欺骗和会话拦截(中间人攻击)

    在无线环境中，非法用户通过侦听等手段获得网络中合法站点的 MAC 地址比有线环境中要容易得多，这些合法的 MAC 地址可以被用来进行恶意攻击。

    另外，由于 IEEE802.11 没有对 WLAN 设备的身份进行认证，非法用户很容易装扮成 WLAN 设备进入网络，并进一步获取合法用户的鉴别身份信息，通过会话拦截实现网络入侵。

  - 高级入侵(企业网)

    一旦攻击者进入无线网络，它将成为进一步入侵其他系统的起点。多数企业部署的 WLAN 都在防火墙之后，这样 WLAN 的安全隐患就会成为整个安全系统的漏洞，只要攻破无线网络，就会使整个网络暴露在非法用户面前。

- 基本的 WLAN 安全技术

  通常网络的安全性主要体现在访问控制和数据加密两个方面。访问控制保证敏感数据只能由授权用户进行访问，而数据加密则保证发送的数据只能被所期望的用户所接收和理解。

  - 物理地址（MAC）过滤

    每个无线客户端网卡都由唯一的 48 位物理地址（MAC）标识，可在 WLAN 服务端中手工维护一组允许访问的 MAC 地址列表，实现物理地址过滤。这种方法的效率会随着终端数目的增加而降低，而且非法用户通过网络侦听就可获得合法的 MAC 地址表，而 MAC 地址并不难修改，因而非法用户完全可以盗用合法用户的 MAC 地址来非法接入。

  - 服务区标识符 (SSID) 匹配

    无线客户端必需设置与无线设备相同的 SSID ，才能访问 WLAN 服务端；如果出示的 SSID 与 WLAN 服务端的 SSID 不同，那么 WLAN 服务端将拒绝它通过本服务区上网。利用 SSID 设置，可以很好地进行用户群体分组，避免任意漫游带来的安全和访问性能的问题。通过设置隐藏接入点（AP）、SSID 区域的划分和权限控制来达到保密的目的。因此可以认为 SSID 是一个简单的口令，通过提供口令认证机制，实现一定的安全。

  - 有线对等保密（WEP）

    在 IEEE802.11 中，定义了 WEP 来对无线传送的数据进行加密，WEP 的核心是采用的 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只有 40 位或 104 位。同时 WEP 还可以作为一种认证方法。

  - 端口访问控制技术（IEEE802.1x）

IEEE802.1x 并不是专为 WLAN 设计的。它是一种基于端口的访问控制技术。

该技术也是用于无线局域网的一种增强网络安全解决方案。当无线工作站 STA 与无线访问点 AP 关联后，是否可以使用 AP 的服务要取决于 802.1x 的认证结果。如果认证通过，则 AP 为 STA 打开这个逻辑端口，否则不允许用户连接网络。

IEEE802.1x 提供 WLAN 客户端与 RADIUS 服务器之间的认证，而不是客户端与无线接入点 AP 之间的认证；采用的用户认证信息仅仅是用户名与口令，在存储、使用和认证信息传递中存在很大安全隐患，如泄漏、丢失；无线接入点 AP 与 RADIUS 服务器之间基于共享密钥完成认证过程协商出的会话密钥的传递，该共享密钥为静态，存在一定的安全隐患。

802.1x 协议仅仅关注端口的打开与关闭，对于合法用户接入时，该端口打开，而对于非法用户接入或没有用户接入时，则该端口处于关闭状态。认证的结果在于端口状态的改变，而不涉及通常认证技术必须考虑的 IP 地址协商和分配问题，是各种认证技术中最简化的实现方案。

在客户端与认证服务器交换口令信息的时候，没有将口令以明文直接送到网络上进行传输，而是对口令信息进行了不可逆的加密算法处理，使在网络上传输的敏感信息有了更高的安全保障，杜绝了由于下级接入设备所具有的广播特性而导致敏感信息泄漏的问题。

- WPA (Wi-Fi Protected Access)

  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/CCMP，WPA=802.1x+EAP/PSK +TKIP/CCMP+MIC。

  - 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，它要求用户必须提供某种形式的证据来证明它是合法用户，并拥有对某些网络资源的访问权，并且是强制性的。
  - 加密：WPA 采用 TKIP/CCMP 为加密引入了新的机制，它使用一种密钥构架和管理方法，通过由认证服务器动态生成分发的密钥来取代单个静态密钥、把密钥首部长度从 24 位增加到 48 位等方法增强安全性。而且，TKIP/CCMP 利用了 802.1x/EAP 构架。认证服务器在接受了用户身份后，使用 802.1x 产生一个唯一的主密钥处理会话。然后，TKIP 把这个密钥通过安全通道分发到 WLAN 设备和客户端，并建立起一个密钥构架和管理系统，使用主密钥为用户会话动态产生一个唯一的数据加密密钥，来加密每一个无线通信数据报文。TKIP/CCMP 的密钥构架使 WEP 静态单一的密钥变成动态密钥。

    TKIP 与 WEP 一样基于 RC4 加密算法，但相比 WEP 算法，将 WEP 密钥的长度由 40 位加长到 128 位，初始化向量 IV 的长度由 24 位加长到 48 位，并对现有的 WEP 进行了改进，即追加了“每发一个包重新生成一个新的密钥(Per Packet Key)”、“消息完整性检查（MIC）”、“具有序列功能的初始向量”和“密钥生成和定期更新功能”四种算法，极大地提高了加密安全强度。

    TKIP 只能作为一种临时的过渡方案，而 IEEE802.11i 标准的最终方案是基于 IEEE802.1x 认证的 CCMP（CBC-MAC Protocol）加密技术，即以 AES（Advanced Encryption Standard）为核心算法。它采用 CBC-MAC 加密模式，具有分组序号的初始向量。CCMP 为 128 位的分组加密算法，相比前面所述的所有算法安全程度更高。
  - 消息完整性校验(MIC)：是为了防止攻击者从中间截获数据报文、篡改后重发而设置的。除了和 802.11 一样继续保留对每个数据分段(MPDU)进行 CRC 校验外，WPA 为 802.11 的每个数据分组(MSDU)都增加了一个 8 个字节的消息完整性校验值，这和 802.11 对每个数据分段(MPDU)进行 ICV 校验的目的不

同。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。而 WPA 中的 MIC则是为了防止黑客的篡改而定制的，它采用 Michael 算法，具有很高的安全特性。当 MIC 发生错误的时候，数据很可能已经被篡改，系统很可能正在受到攻击。此时，WPA 还会采取一系列的对策，比如立刻更换组密钥、暂停活动等，来阻止黑客的攻击。

- IEEE 802.11i

  为了进一步加强无线网络的安全性和保证不同厂家之间无线安全技术的兼容，IEEE802.11 工作组开发了作为新的安全标准的 IEEE802.11i 。IEEE 802.11i 标准中主要包含加密技术：TKIP(Temporal Key Integrity Protocol)和 AES（Advanced Encryption Standard），以及认证协议：IEEE802.1x 。

  说明

  1. AES: 更好的加密算法，但是无法与原有的 802.11 架构兼容，需要硬件升级。
  2. CCMP 和 TKIP: 以 AES 为基础。
  3. IBSS: 802.11i 解决 IBSS （Independent Basic Service Set）, 而 WPA 主要处理 ESS （Extended Service Set）。
  4. Pre authentication: 用于用户在不同的 BSS（Basic Service Set）间漫游时，减少重新连接的时间延迟。

  - 认证：802.11i 的安全体系也使用 802.1x 认证机制，通过 WLAN 客户端与 radius 服务器之间动态协商生成 PMK(Pairwise Master Key)，再由 WLAN 客户端和 WLAN 服务端之间在这个 PMK 的基础上经过四次握手协商出单播密钥以及通过两次握手协商出组播密钥，每一个 WLAN 客户端与 WLAN 服务端之间通讯的加密密钥都不相同，而且会定期更新密钥，很大程度上保证了通讯的安全。
  - 加密：高安全的 CCMP 加密算法。

1.4.11 WLAN QoS

WLAN QoS 保证不同质量的无线接入服务之间的互通，满足实际应用的需求。

802.11 网络提供了基于竞争的无线接入服务，但是不同的应用需求对于网络的要求是不同的，而原始的网络不能为不同的应用提供不同质量的接入服务，所以已经不能满足实际应用的需要。考虑到基于时间的数据传输的 QoS 重要性，在 IEEE 正式批准 802.11e 标准之前，已经有一些无线设备制造商开始在实施能基本满足近期需要的 QoS 机制，这些大都是基于 EDCF 的，最有代表性的就是 Wi-Fi 联盟的 WMM。WMM 并不是一个新的标准，它实际上是 802.11e 的一个子集，802.11e 是基于 802.1p 的八级优先级结构，但 Wi-Fi 联盟的 WMM 规范则只规定了四级 WMM 优先级，按优先级从高到低依次是语音（Voice）、视频（Video）、尽力而为（Best Effort）、背景（Background）等。802.11e 的优先级方案基本与此相同，只不过它用到了 802.1p 里定义的所有八个优先级而不像 WMM 那样只用到了一个子集。

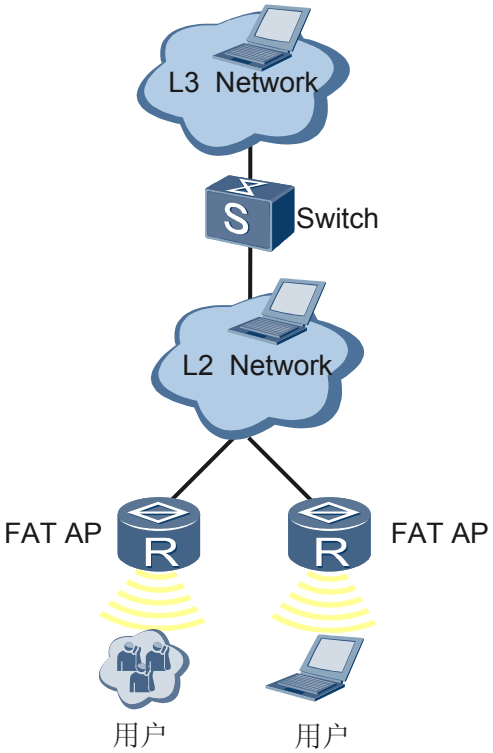
一个具有 QoS 的网络系统需要三个方面的共同支持，它们分别是源点（服务端）、网络和终点（客户端），而每一方面都必须要支持 QoS 才行，开放系统互联协议有七层，对于 QoS 来说，主要关心数据链路层和应用层。WLAN QoS 的设计与实现主要发生在数据链路层。从更上层的协议级别实现 QoS 当然也可行，但从数据链路层入手是一个更好的解决方案，很多设备可以很快地在这个级别上分析数据包中和 QoS 相关的头部信息。

现在已经出现了能支持 802.11e 和 WMM 的无线网络硬件，但是由于标准的滞后，各个厂商的设备之间很难保证在 QoS 方面互通，因此，到目前为止部署具有服务质量保证的大型无线局域网还是一件非常困难的工作。

1.5 应用

1.5.1 AR1200 为无线接入点

图 1-12 AR1200 为无线接入点



如图 1-12 所示，AR1200 作为无线接入和控制点，控制 WLAN 用户的接入和认证过程，完成用户数据加密、用户认证、QoS 等功能。

1.6 术语与缩略语

缩略语

缩略语	英文全称	中文全称
AES	advanced encryption standard	高级加密标准（美国国家标准与技术协会制定的用以替代 DES 的加密算法）
AP	Access Point	接入点,是指任何一个能通过无线介质为无线终端提供分布式访问服务的实体

缩略语	英文全称	中文全称
AS	Authentication Server	认证服务器
ASU	Authentication Server Unit	认证服务器，用于对用户和设备证书进行身份鉴别等，是基于公钥密码技术的 WAI 中重要的组成部分
BK	Base Key	基密钥用于导出单播会话密钥，由证书鉴别过程协商得到或者由预共享密钥导出
BSS	Basic Service Set	基础服务集
CCMP	CTR with CBC-MAC Protocol	计数器模式及密码块链消息认证码协议
EAP	Extensible Authentication Protocol	可扩展认证协议
EAPOL	Extensible Authentication Protocol over LAN	承载在 LAN 上的 EAP
ESS	Extended Service Set	扩展服务集
FAT AP	FAT Access Point	胖 AP，传统 AP，除了提供基本的无线连接功能外，还能提供安全、管理和性能增强功能。FAT AP 不能与 AC 关联使用
FIT AP	FIT Access Point	瘦 AP 区别于传统的 FAT AP，只提供可靠、高性能的无线连接功能，而剥离了其它功能
GTK	group temporal key	组临时密钥
MSK	Multicast Session Key	组播会话密钥用于保护站点发送的组播 报文的随机值，由组播主密钥导出，包括组播加密密钥和组播完整性校验密钥。
PSK	Preshared Key	预共享密钥是发布给 STA 的静态密钥
STA	Station	站点即无线终端
USK	Unicast Session Key	单播会话密钥是由 BK 通过伪随机函数导出的随机值，分为四个部分：单播加密密钥、单播完整性校验密钥、消息鉴别密钥和密钥加密密钥
MIC	message integrity code	MAC 完整性校验码
PMK	pairwise master key	成对主密钥
PTK	pairwise transient key	成对临时密钥
RADIUS	Remote Authentication Dial-In User Service	远程认证拨号用户服务
RSN	robust security network	健壮的安全网络

缩略语	英文全称	中文全称
RSNA	robust security network association	健壮的安全网络关联
TKIP	Temporal Key Integrity Protocol	暂时密钥完整性协议
WAPI	WLAN Authentication and Privacy Infrastructure	无线局域网鉴别和保密基础结构
WPA	Wi-Fi Protected Access	Wi-Fi 网络安全存取
WEP	Wired Equivalent Privacy	有效等效加密