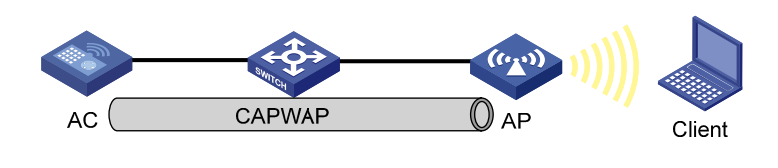
**CAPWAP协议**

**介绍**

CAPWAP(Controlling and Provisioning of Wireless Access Point，无线接入点的控制和配置)协议定义了AP与AC之间如何通信，为实现AP和AC之间互通性提供一个通用封装和传输机制，如下图所示



CAPWAP同时运行在AP和AC上，为WLAN系统提供安全的AC与AP之间的通信。AP与AC之间的通信依照标准UDP客户端/服务器端模型来建立。

CAPWAP提供数据隧道来封装发往AC的数据包。这些数据包可以是802.11协议的数据包。CAPWAP还支持AC的远程AP配置、WLAN管理和漫游管理。在AC上，CAPWAP提供了AP管理功能、AC可以根据管理员提供的信息动态的配置AP。协议支持local MAC和split MAC两种模式，下图1为local MAC模式下，WTP对无线帧进行处理，然后封装成IEEE802.3帧转发到AC；而在split MAC模式下，无线帧直接被WTP封装转发到AC，如下图2所示。

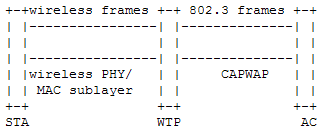


图1

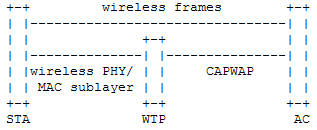


图2

在IP网络中CAPWAP使用UDP协议作为承载协议，支持IPv4和IPv6协议，接入点可以动态的选择使用IPv4或者IPv6和AC建立链接。因此，CAPWAP支持IPv4和IPv6协议可以更好的支持在后续网络改造中，所有的AP和AC、都不需要升级就可以继续提供WLAN接入服务，极大方便了网络建设和维护，保证用户的投资回报。

**技术术语**

**Access Controller (AC):**在数据层面、控制层面、管理层面提供WTP访问基础网络的实体。

**CAPWAP Control Channel:**在AC与WTP之间建立的基于UDP协议的控制管理通道。

**CAPWAP Data Channel：**在AC与WTP之间建立的基于UDP协议的数据传输通道。

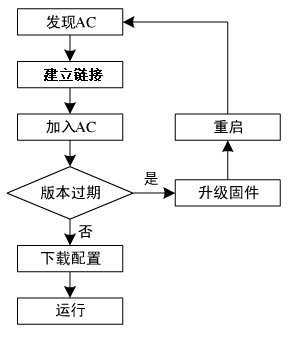
**Station（STA）:** 可以访问无线网络的实体或设备。

**Wireless Termination Point（WTP）:**无线终端。

**工作原理**

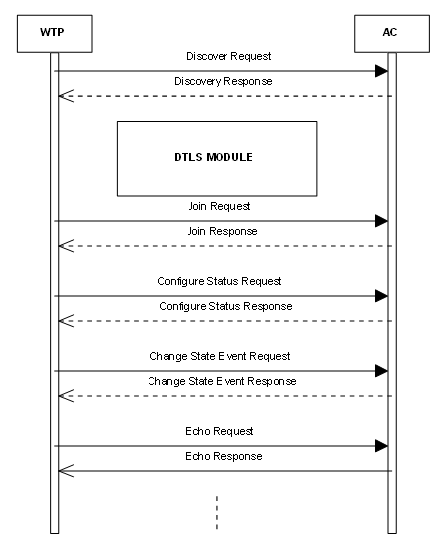
WTP被链接到网络时即进入发现AC的过程。WTP使用广播、组播或单播方式发送“发现请求”，当使用单播方式时，需首先通过DHCP或DNS获得AC的IP地址列表。收到请求的AC返回“发送应答”给WTP，WTP在应答的AC中，选择一个建立链接。

当链接建立成功后，WTP发送“加入请求”，AC回复“加入应答”确认WTP加入该AC的管理范围。若WTP的固件版本过期，则进入升级固件过程，WTP从AC下载最新版本的固件，升级成功后重启，重新进入发现过程；若WTP固件为新版本，则从AC下载配置参数，随后进入运行状态。下图为CAPWAP工作原理示意图：



在运行状态中，AC通过控制报文动态更改WTP配置，获取WTP运行状态、STA信息、射频信息等，由于所有数据都集中在AC进行处理，因此可以容易实施全网级QoS、动态射频管理等策略。

下图是CAPWAP在AC、WTP之间的信息交互过程：

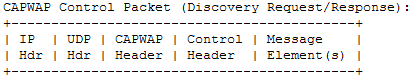


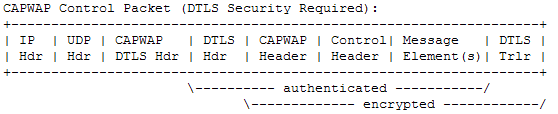
* **Discovery的状态：**发现AC上报自己的信息，SN，MAC，apcode，versioncode，softversion,aptype.等信息。,从Request中获取Acname，ACip，AC的接入STA限制数等。
* **Join状态：**上报wtp的更多基本信息，radio个数，ip地址，WTP支持的数据转发类型等信息，AC也会给AP回复更多的AC的相关信息，比如接入的活跃的WTP数等。在Join状态建立capwap控制通道。
* **ImageData状态：**是AP的升级态，目前我们的升级策略是WTP在Jion结束时发现softversion和AC回复的不同，进入ImageData状态，在这个状态有两次交互，第一次交互，WTP获取到tftp路径，开始从AC上tftp升级文件，第二次交互，是WTP完成下载后给AC发Response，没什么内容，就是告诉AC我下载完成了，AC再给WTP发Reset Request， WTP收到后进入Reset状态，发送Reset Response 然后进入烧写升级过程。
* **Config状态：**WTP从AC获取一些radio级别的参数，保存，等到RUN状态创建wlan的时候使用。
* **Datacheck状态：**创建数据通道，打开控制通道的心跳线，也就是开始发送echo报文，10秒发送一个。
* **RUN状态：**IEEE802.11wlan 类型的报文负责创建wlan，updateconfig类型的报文负责修改radio的属性。StationConfigration类型的报文负责sta的接入和删除。RUN状态的超时是1分钟收不到任何包就QUIT，每次收到包会重置定时器，echo的定时期也会被同时重置。SPEC\_PAYLOAD类型的报文负责上报给AC，WTP收到的相关信息。

**报文结构**

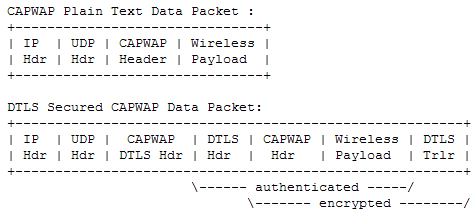
CAPWAP协议规定AC和WTP的通信分为控制报文和数据报文，控制报文只在AC和WTP之间传输，实现配置、管理、监控等功能；数据报文则是将被转发的用户数据帧。2种报文通过不同的UDP端口进行传输(控制报文port: 32768,数据报文port: 32769)，控制报文中除”发现请求/应答”是明文传输外，其它的强制使用DTLS保护，而数据报文可选择是否使用DTLS。报文结构如下图所示：

控制报文：

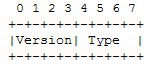




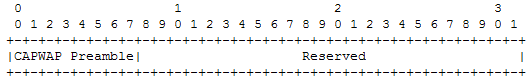
数据报文：



其中两种报文中的CAPWAP首部的前8位是前导码，用于快速判断此报文是否经过DTLS加密。前4位指明CAPWAP版本，目前版本号为0；后4位值为1时时CAPWAP DTLS首部，值为0时时CAPWAP首部。其格式为下图：

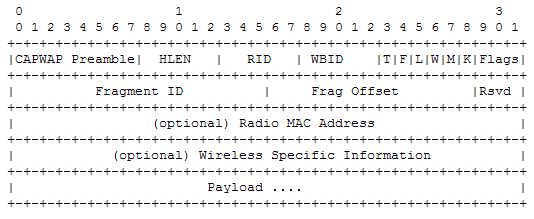
****

CAPWAP DTLS 首部如下图所示：

****

该字段标识此报文经过DTLS加密。长度为32位，包括8位前导码，在控制信道收到此报文则是控制报文，在数据信道收到则是数据报文。

下图是CAPWAP首部的结构：

****

**CAPWAP preamble：**前四位表示CAPWAP的版本信息，后四位如果是0就是不加密的报文，如果是1就是加密的报文

**HLEN：**capwap头的长度

**RID：**radio ID

**WBID：**wireless binding id

**T：**传输的报文的格式，1表示负载为由WBID定义的类型，0表示负载为802.3帧。

**F：**当前报文是否分片。1表示当前报文是分片。

**L：**只有F标志置位才有效。1表示是最后一个分片，0表示后面还有分片。

**W：**表示optional Wireless Specific Information字段是否存在，1为存在。

**M：**表示Radio MAC Address optional是否存在。

**K：**表示是否是数据通道的keep-alive包。

**Flags：**保留字段。

**Fragment ID：**分片时标识每个分片的序列号。

**Fragment Offset：**分片时标识每个分片的偏移（8字节为单位）。

**Reserved：**保留字段。

**Radio MAC Address：**当报文中是802.3帧时保留wtp的mac。

**Wireless Specific Information：**无线扩展信息。

**参考文献：**

1. **RFC5415**
2. **技术交流文档**
3. **网络**