本文翻译者：weicq2000(weicq2000@sina.com，2013 年 7 月 4 日译)

Network Working Group
Request for Comments: 5415
Category: Standards Track

P. Calhoun, Ed.
Cisco Systems, Inc.
M. Montemurro, Ed.
Research In Motion
D. Stanley, Ed.
Aruba Networks
March 2009

无线 AP 控制和配置(CAPWAP)协议标准

本备忘录状态

本文档规定互联网通信的互联网标准跟踪协议，并请求讨论和提出改进建议。本协议的标准化程度和状态，参阅“Internet Official Protocol Standards”(STD 1)的目前版本。分发本备忘录不受限制。

摘要

本规范定义无线 AP 控制和配置(Control And Provisioning of Wireless Access Points, CAPWAP)协议，满足在 RFC4564 中由 CAPWAP Working Group 定义的目标。CAPWAP 协议在设计上颇具灵活性，这使其能够用于各种无线技术。本文档介绍基础 CAPWAP 协议，而独立的绑定扩展使其可与其他无线技术一起使用。

目录

4-6-17 解密错误报告
4-6-18 解密错误报告周期
4-6-19 删除MAC ACL条目
4-6-20 删除站
4-6-21 发现类型
4-6-22 重复的IPv4地址
4-6-23 重复的IPv6地址
4-6-24 空闲超时
4-6-25 ECN支持
4-6-26 映像数据
4-6-27 映像标识符
4-6-28 映像信息
4-6-29 启动下载
4-6-30 位置数据
4-6-31 最大消息长度
4-6-32 MTU发现填充
4-6-33 无线电设备管理状态
4-6-34 无线电设备运行状态
4-6-35 结果代码
4-6-36 返回的消息要素
4-6-37 会话ID
4-6-38 统计量计时器
4-6-39 特定供应商净荷
4-6-40 WTP 主板(Board)数据
4-6-41 WTP描述符
4-6-42 WTP回退
4-6-43 WTP帧隧道模式
4-6-44 WTP MAC类型
4-6-45 WTP名称
4-6-46 WTP无线电设备统计量
4-6-47 WTP重启统计量
4-6-48 WTP静态IP地址信息
4-7 CAPWAP 协议计时器
4-7-1 ChangeStatePendingTimer
4-7-2 DataChannelKeepAlive
4-7-3 DataChannelDeadInterval
4-7-4 DataCheckTimer
4-7-5 DiscoveryInterval
4-7-6 DTLSSessionDelete
4-7-7 EchoInterval
4-7-8 IdleTimeout
4-7-9 ImageDataStartTimer
4-7-10 MaxDiscoveryInterval
4-7-11 ReportInterval

第 1 章　序言

这个文档介绍 CAPWAP 协议，一个标准的、互操作协议，它使接入控制器(Access Controller, AC)能够管理无线终端点(Wireless Termination Points, WTPs)的集合。CAPWAP 协议的定义与层 2(L2)技术无关，满足在“无线接入点的控制和配置目标(Objectives for Control and Provisioning of Wireless Access Points (CAPWAP))”[RFC4564]中的目标。

集中式 IEEE 802.11 无线局域网(Wireless Local Area Network, WLAN)架构的出现，该架构中 IEEE 802.11 WTPs 由 AC 轻松管理，暗示基于标准的、可互操作的协议能够极大简化无线网络部署和管理。WTPs 需要一系列动态管理和控制功能，这些功能与 WTPs 连接无线和有线媒介的主要任务有关。管理 WTPs 的传统协议或者是通过 HTTP、通过特定第 2 层专有方法人工静态配置，或者就根本没有(如果 WTPs 是自组织的)。在[RFC5416]中定义的 IEEE 802.11 绑定，用于支持 CAPWAP 协议与 IEEE 802.11 WLAN 网络一起应用。

CAPWAP 假设，网络被配置成由通过 IP(Internet Protocol)与 AC 通信的多个 WTPs 构成。WTPs 被看作是由 AC 控制的远端无线电设备射频(Radio Frequency, RF)接口。CAPWAP 协议支持两种运行模式：Split MAC(Medium Access Control)和 Local MAC。在 Split MAC 运行模式，所有第 2 层无线数据和管理帧由 CAPWAP 协议封装，并在 AC 和 WTP 间交换。如

图 1 所示，从移动设备(本规范将移动设备称为站(Station, STA))收到的无线帧，直接由 WTP 封装并转发到 AC。

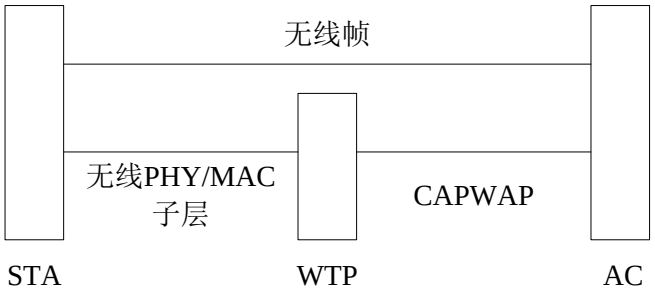


图 1　典型 Split MAC CAPWAP 架构

Local MAC 运行模式可用于本地桥接的数据帧，或用于隧道化为 802.3 帧的数据帧。后者暗示 WTP 执行 802.11 Integration 功能。在每一种情况，第 2 层无线管理帧由 WTP 在本地处理，接着转发到 AC。图 2 显示 Local MAC 模式，在该模式中，站发射无线帧，该无线帧用 802.3 帧封装，并被转发到 AC。

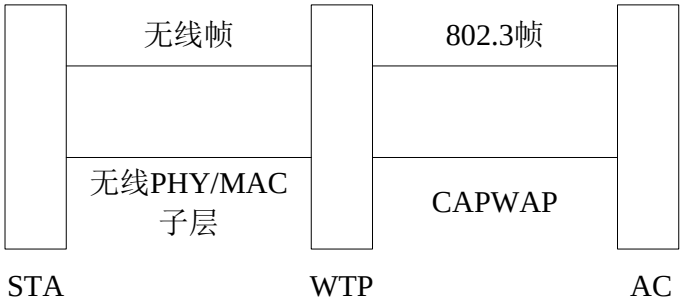


图 2　典型 Local MAC CAPWAP 架构

提供具有安全证书的 WTPs 和决定授权哪个 WTPs 提供业务，传统通过专用解决方案处理。允许以可互操作的方式、从集中的 AC 执行这些功能增加了可管理性，使网络运营商能够更严密控制他们的无线网络基础架构。

1-1　目标

CAPWAP 协议的目标是：

1、为了集中无线网络的认证功能和策略执行功能。AC 也可以提供集中的桥接、转发和用户流量加密。通过在无线网络更多使用网络处理芯片能力，类似有线 LANs 经历的：集中这些功能将降低成本，提高效率。

2、为了能够将较高层协议处理从 WTP 转出。把时间敏感的无线控制应用和接入应用留在 WTP，从而提高 WTPs 中有限计算能力的使用效率，这些应用现在受到严重成本压力。

3、为了提供不受限于特定无线技术的可扩展协议。采用通用的封装和传输机制获得可扩展性，使得将来通过特定无线绑定， CAPWAP 协议能够用于许多接入点类型。

CAPWAP 协议仅关注 WTP 和 AC 间的接口。AC 间和站到 AC 的通信严格讲超出这个文档范围。

1-2　本文档中的约定

本文档中出现的术语“MUST”、“MUST NOT”、“REQUIRED”、“SHALL”、“SHALL NOT”、“SHOULD”、“SHOULD NOT”、“RECOMMENDED”、“MAY”和“OPTIONAL”的含义，遵循RFC 2119[RFC2119]描述。

1-3 特约作者

这一节呈上对本标准重要内容和概念做出贡献的作者，并向他们致谢。

CAPWAP Working Group 选择 Lightweight Access Point Protocol (LWAPP) [LWAPP]为 CAPWAP 协议规范的基础。LWAPP 文档的作者为：

Bob O’Hara
Email: bob.ohara@computer.org

Pat Calhoun, Cisco Systems, Inc.
170 West Tasman Drive, San Jose, CA 95134
Phone: +1 408-902-3240, Email: pcalhoun@cisco.com

Rohit Suri, Cisco Systems, Inc.
170 West Tasman Drive, San Jose, CA 95134
Phone: +1 408-853-5548, Email: rsuri@cisco.com

Nancy Cam Winget, Cisco Systems, Inc.
170 West Tasman Drive, San Jose, CA 95134
Phone: +1 408-853-0532, Email: ncamwing@cisco.com

Scott Kelly, Aruba Networks
1322 Crossman Ave, Sunnyvale, CA 94089
Phone: +1 408-754-8408, Email: skelly@arubanetworks.com

Michael Glenn Williams, Nokia, Inc.
313 Fairchild Drive, Mountain View, CA 94043
Phone: +1 650-714-7758, Email: Michael.G.Williams@Nokia.com

Sue Hares, Green Hills Software
825 Victors Way, Suite 100, Ann Arbor, MI 48108
Phone: +1 734 222 1610, Email: shares@ndzh.com

Datagram Transport Layer Security (DTLS) [RFC4347]被用作 CAPWAP 协议的安全解决方案。本文档中与 DTLS 有关的重要内容的作者为：

Scott Kelly, Aruba Networks
1322 Crossman Ave, Sunnyvale, CA 94089
Phone: +1 408-754-8408
Email: skelly@arubanetworks.com

Eric Rescorla, Network Resonance
2483 El Camino Real, #212,Palo Alto CA, 94303
Email: ekr@networkresonance.com

DTLS 概念的使用确保 CAPWAP 协议成为 Secure Light Access Point Protocol (SLAPP)建议 [SLAPP]的一部分。SLAPP 建议的作者为：

Partha Narasimhan, Aruba Networks
1322 Crossman Ave, Sunnyvale, CA 94089
Phone: +1 408-480-4716
Email: partha@arubanetworks.com

Dan Harkins, Trapeze Networks
5753 W. Las Positas Blvd, Pleasanton, CA 94588
Phone: +1-925-474-2212
EMail: dharkins@trpz.com

Subbu Ponnuswamy, Aruba Networks
1322 Crossman Ave, Sunnyvale, CA 94089
Phone: +1 408-754-1213
Email: subbu@arubanetworks.com

为撰写[RFC5418]文档所涉及安全部分内容作出重要贡献的人士有：

T. Charles Clancy, Laboratory for Telecommunications Sciences,
8080 Greenmead Drive, College Park, MD 20740
Phone: +1 240-373-5069, Email: clancy@ltsnet.net

Scott Kelly, Aruba Networks
1322 Crossman Ave, Sunnyvale, CA 94089
Phone: +1 408-754-8408, Email: scott@hyperthought.com

1-4 术语

- Access Controller (AC)
  访问控制。在数据平面、控制平面、管理平面，或它们的组合中，将 WTP 接入到网络基础设施的网络实体。
- CAPWAP Control Channel
  CAPWAP 控制通道。由 AC IP Address、WTP IP Address、AC 控制端口、WTP 控制端口和传输层协议(UDP 或 UDP-Lite)定义的双向流，在其上发送和接收 CAPWAP Control 分组。
- CAPWAP Data Channel
  CAPWAP 数据通道。由 AC IP Address、WTP IP Address、AC 数据端口、WTP 数据端口和传输层协议(UDP 或 UDP-Lite)定义的双向流，在其上发送和接收 CAPWAP Data 分组。

- Station (STA)

  站(STA)。包含到无线媒介(Wireless Medium, WM)接口的设备。

- Wireless Termination Point (WTP)

  无线终端点(WTP)。包括射频天线和无线物理层(PHY)的物理或网络实体，主要功能是发送和接收无线接入网络的站流量。

  本文档使用[RFC3753]中定义的补充术语。

第 2 章　协议综述

CAPWAP 协议是通用协议，它定义通过 CAPWAP 协议传输机制，进行 AC 和 WTP 控制和数据平面通信。CAPWAP Control 消息，和可选的 CAPWAP Data 消息，使用 Datagram Transport Layer Security(DTLS) [RFC4347]进行安全保护。DTLS 是源于 TLS 的标准跟踪 IETF 协议。TLS 的基础安全相关协议机制已经成功部署许多年。

CAPWAP 协议传输层携带两类净荷，CAPWAP Data 消息和 CAPWAP Control 消息。CAPWAP Data 消息封装转发的无线帧。CAPWAP Control 消息是 WTP 和 AC 间交换的管理消息。CAPWAP Data 分组和 Control 分组在分开的 UDP 端口上发送。因为数据分组和控制分组可能都超过 Maximum Transmission Unit (MTU)长度，CAPWAP Data 或 Control 消息的净荷可能需要分段。第 3 章定义分段处理。

CAPWAP Protocol 由 Discovery 阶段开始。WTPs 发送 Discovery Request 消息，诱发任何收到该消息的 AC 用 Discovery Response 消息响应。根据收到的 Discovery Response 消息，WTP 用与其建立安全的 DTLS 会话来选择一个 AC。为了建立安全的 DTLS 连接，WTP 需要做某些预配置，预配置在第 12-5 节介绍。根据发现的、网络能支持的最大长度，分段 CAPWAP 协议消息。

一旦 WTP 和 AC 完成 DTLS 会话建立，开始配置交换，其间两个设备对采用的版本达成一致。在这个交换中，WTP 可以接收配置设置。然后，WTP 开始运行。

当 WTP 和 AC 完成版本和配置交换并启动 WTP 后，CAPWAP 协议用于封装在 WTP 和 AC 见发送的无线数据帧。如果被封装的无线用户数据(Data)帧或协议控制(Management)帧的长度引起最终的 CAPWAP 协议分组超过 WTP 和 AC 间支持的 MTU，CAPWAP 协议将分段第 2 层帧。为了重建原始封装的净荷，被分段的 CAPWAP 分组被重组。MTU Discovery and Fragmentation 在第 3 章介绍。

~~CAPWAP Protocol 由 Discovery 阶段开始。WTPs 发送 Discovery Request 消息，诱发任何收到该消息的 AC 用 Discovery Response 消息响应。根据收到的 Discovery Response 消息，WTP 用与其建立安全的 DTLS 会话来选择一个 AC。为了建立安全的 DTLS 连接，WTP 需要一些预配置，预配置在第 12-5 节介绍。根据发现的、网络能支持的最大长度，分段 CAPWAP 协议消息。~~

~~一旦 WTP 和 AC 完成 DTLS 会话建立，开始配置交换，其间两个设备对采用的版本达成一致。在这个交换中，WTP 可以接收配置设置。然后，WTP 开始运行。~~

~~当 WTP 和 AC 完成版本和配置交换并启动 WTP 后，CAPWAP 协议用于封装在 WTP 和 AC 间发送的无线数据帧。如果被封装的无线用户数据(Data)帧或协议控制(Management)帧的长度引起最终的 CAPWAP 协议分组超过 WTP 和 AC 间支持的 MTU，CAPWAP 协议将分段第 2 层帧。为了重建原始封装的净荷，分段的 CAPWAP 分组被重组。MTU Discovery and Fragmentation 在第 3 章介绍。~~

CAPWAP 协议提供从 AC 到 WTP 的指令传送，这些指令用于管理与 WTP 通信的站。这可以包括在 WTP 中建立这些站的本地数据结构，以及收集有关 WTP 与这些站间通信的统计信息。CAPWAP 协议为 AC 提供机制，以便获得由 WTP 收集的统计信息。

CAPWAP 协议提供保持激活(keep-alive)功能，该功能保持 WTP 和 AC 间的通信信道。如果该 AC 没有显现激活，WTP 将尝试发现新的 AC。

2-1 无线绑定定义

CAPWAP 协议与特定 WTP 无线电设备技术无关，也与它的相关无线链路层协议无关。CAPWAP 协议的各个部分采用标准方法设计，适应每一种无线技术的特定需要。具体无线技术采用的 CAPWAP 协议**必须**遵循为那个技术定义的绑定要求。

定义无线技术绑定时，编写者**必须**包括任何特定技术消息的必要定义，以及所有这些消息的特定技术消息要素(message elements)。最低限度，绑定**必须**提供：

1、在 WTP Event Request 消息中携带的、特定绑定 Statistics 消息要素的定义。

2、在 Station Configuration Request 消息中携带的，在 WTP 上配置站信息的消息要素。

3、在 Discovery、Primary Discovery 以及 Join Request 和 Response 消息中携带的，指出在 WTP 和 AC 中支持的特定绑定无线电设备类型的 WTP Radio Information 消息要素。

如果对于本标准中定义的任何现有 CAPWAP 消息要求有特定技术消息要素，这些消息要素也**必须**在技术绑定文档中定义。

特定绑定消息要素的命名**必须**以技术类型名称开始，例如，IEEE 802.11 绑定，在[RFC5416]中提供，以“IEEE 802.11”开始。

CAPWAP绑定概念也**必须**在任何将来的规范中使用，这些将来的规范将功能添加到基本CAPWAP协议规范，或者添加到任何发布的CAPWAP绑定规范。**必须**生成独立的WTP Radio Information消息要素，以便适当通告对规范的支持。这个机制为将来协议扩展做好准备，在提供必要能力通告的同时，通过WTP Radio Information要素，确保WTP/AC可互操作。

2-2 CAPWAP 会话建立综述

本节介绍 CAPWAP WTP 和 AC 间会话建立处理消息交换。带注释梯形图显示 AC 在右边，WTP 在左边，并假设使用 DTLS 认证证书。CAPWAP 协议状态机在第 2-3 节详细介绍。注意，DTLS 允许将一定数量消息聚合到单一帧，这在图 3 中用星号表示。

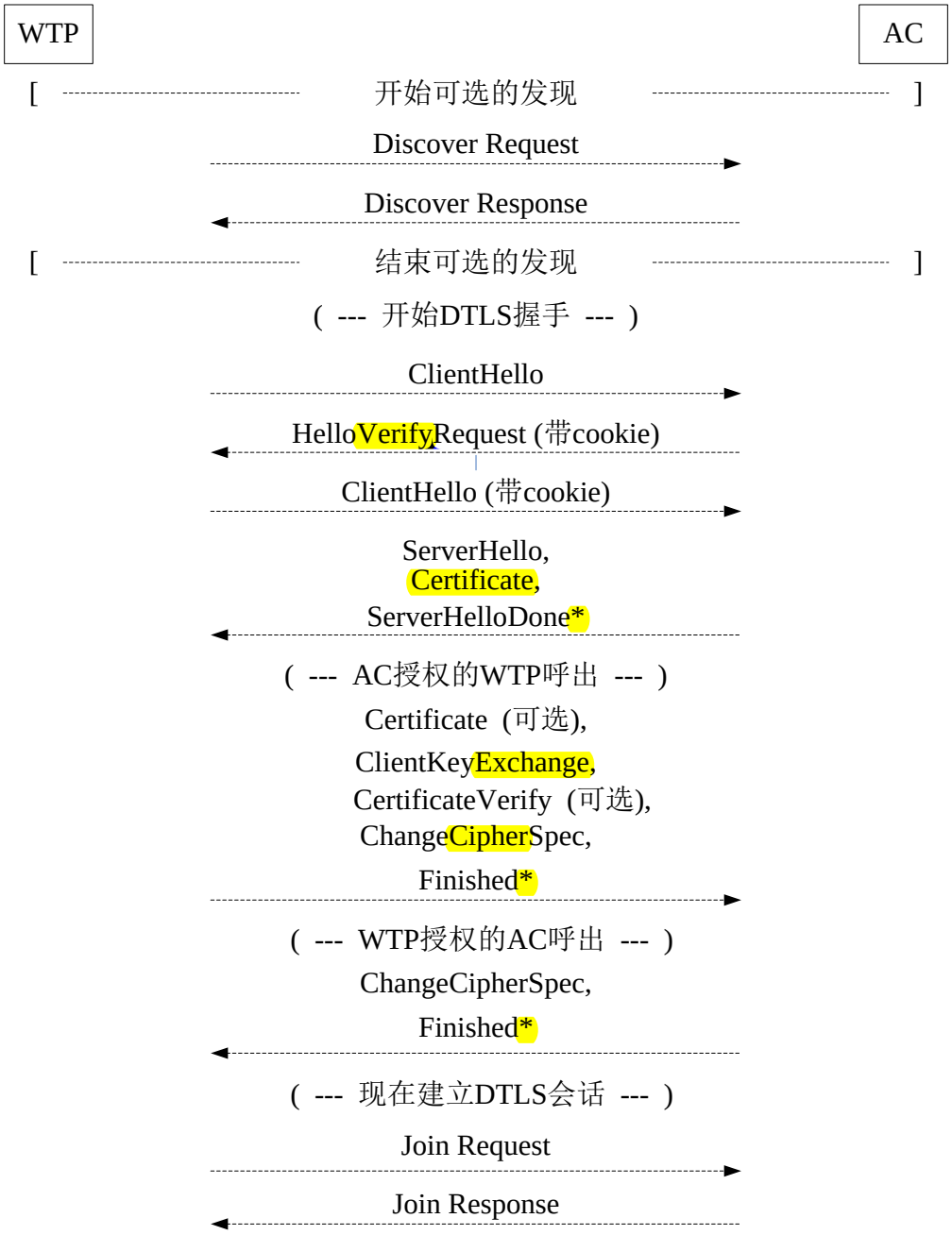


图 3　CAPWAP 控制协议交换

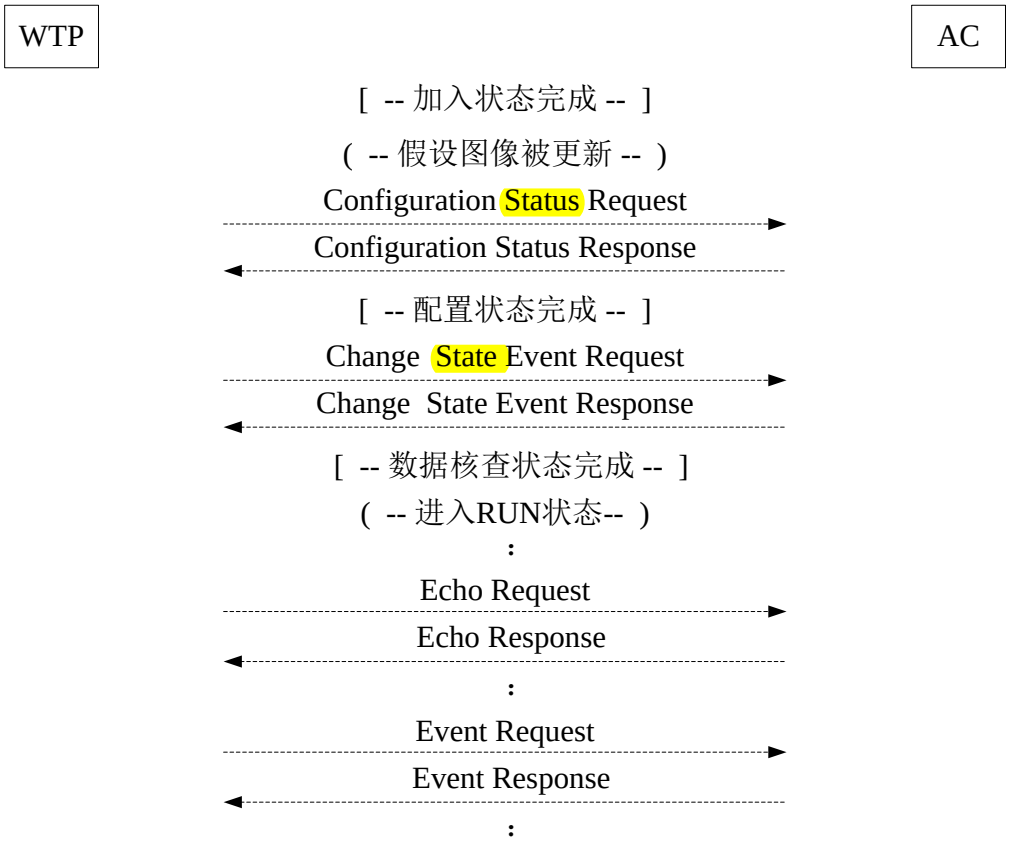


图 3 续　CAPWAP 控制协议交换

在上图所示的 CAPWAP 消息交换末尾，AC 和 WTP 正在安全交换 CAPWAP Control 消息。这个图示用于澄清协议操作，不包括任何可能的错误条件。第 2-3 节详细介绍相应状态机。

2-3　CAPWAP 状态机定义

下述状态图表示 WTP-AC 会话生命周期。由于 CAPWAP 协议使用 DTLS，导致两个名义上独立然而紧密绑定的状态机并置。通过由指令(参阅第 2-3-2-1 节)和通知(参阅第 2-3-2-2 节)构成的 API，DTLS 状态机和 CAPWAP 状态机耦合在一起。CAPWAP 状态机的某些指令触发 DTLS 状态机中的某些转换，而 DTLS 状态机中的某些通知触发 CAPWAP 状态机中的某些转换。

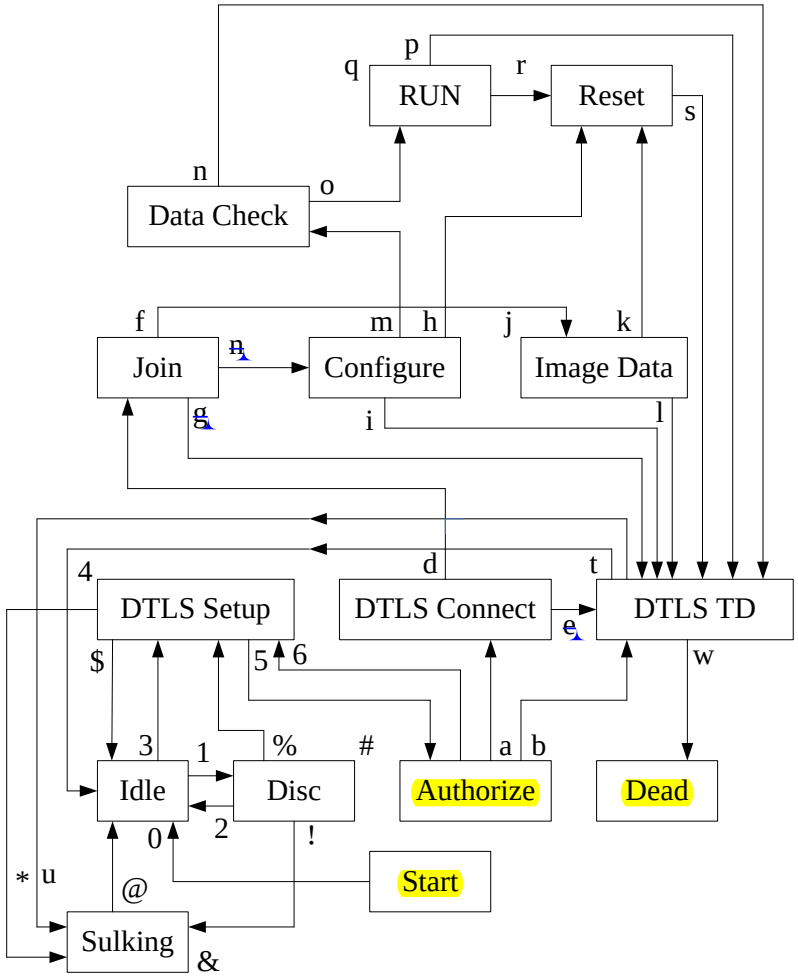


图 4　CAPWAP 集成的状态机

如上所述，CAPWAP 协议状态机由 AC 和 WTP 使用。如果是这些状态不被共享情况(即，AC 或 WTP 的一方或另一方没有执行)，在下面介绍的转换中会显式标出。对于每一种定义的状态，仅准许发送和接收某些消息。状态由 CAPWAP Control 消息定义规定，在这些状态中每个消息是合法的。

因为 WTP 仅与单个 AC 通信，WTP 仅有单个 CAPWAP 状态机实例。在 AC 上状态机的工作与此不同，因为 AC 与许多 WTPs 通信。AC 使用 3 个线程概念。注意，这里使用线程术语没有暗示实现必须使用线程，但是它是实现 AC 状态机的一种可选方法。

Listener Thread：AC 的 Listener 线程通过 DTLSListen 指令，处理入境 DTLS 会话建立请求。创建后，Listener 线程在 DTLS Setup 状态中启动。一旦 DTLS 会话通过验证(当状态机进入“Authorize”状态时发生)，Listener 线程创建 WTP 特定会话 Service 线程和状态上下文。在图 4 中这些状态机转换由数字表示。AC 必须保护自己，抵御存在于未认证帧的各种攻击。更多信息参阅第 12 章。

Discovery Thread：AC 的 Discovery 线程负责接收和响应 Discovery Request 消息。在图 4 中这些状态机转换由数字表示。注意，Discovery 线程不保留任何每个 WTP 特定上下文信息，并且单个状态上下文存在。AC 必须保护自己，抵御存在于未认证帧的各种攻击。更多信息参阅第 12 章。

Service Thread：AC 的 Service 线程处理每个 WTP 状态，并且每个 WTP 连接有一个这

样的线程。这个线程由 Listener 线程在达到 Authorize 状态时创建。创建时，Service 线程继承来自 Listener 线程的状态机上下文副本。当与 WTP 的通信完成时，Service 线程终止并且释放所有关联的资源。图 4 中这些状态机转换由字母和标点符号表示。

第 2-3-1　CAPWAP 协议状态转换

本节介绍各种状态机，以及诱发它们的事件。本节不讨论特定 DTLS 状态和特定 CAPWAP 状态间的互动。这些互动，以及 DTLSspecific 状态和转换，在第 2-3-2 节讨论。

Start 到 Idle (0)：一旦设备初始化完成，这个转换发生。

WTP：这个状态转换用于启动 WTP 的 CAPWAP 状态机。

AC：　AC 创建 Discovery 线程和 Listener 线程，并启动 CAPWAP 状态机。

Idle 到 Discovery (1)：为了支持 CAPWAP 发现处理，这个转换发生。

WTP：在传送第一个 Discovery Request 消息前 WTP 进入 Discovery 状态(参阅第 5-1 节)。一旦进入这个状态，WTP 设置 DiscoveryInterval 计时器(参阅第 4-7 节)。WTP 重新设置 DiscoveryCount 计数器到 0(参阅第 4-8 节)。WTP 也清除在前一个 Discovery 阶段它可能收到的、来自 ACs 的所有信息。

AC：　这个状态转换由 AC 的 Discovery 线程执行，当收到 Discovery Request 消息时发生。AC **应当**用 Discovery Response 消息响应(参阅第 5-2 节)。

Discovery 到 Discovery (#)：在 Discovery 状态，WTP 决定连接到哪一个 AC。

WTP：当 DiscoveryInterval 计时器到期，这个转换发生。如果 WTP 由一组 ACs 配置，WTP 传送 Discovery Request 消息到每个 AC(WTP 还没有从该 AC 收到 Discovery Response 消息)。这个事件每转换一次，WTP 都增加 DiscoveryCount 计数器。关于 WTP 如何知道这些 ACs 是它应当发送 Discovery Request 消息去的 ACs 的更多介绍参阅第 5-1 节。只要 WTP 传送 Discovery Request 消息，WTP 就重新启动 DiscoveryInterval 计时器。

AC：　对于 AC，这是不合法的状态转换。

Discovery 到 Idle (2)：当 Discovery 处理完成，这个转换在 AC 的 Discovery 线程上发生。

WTP：对于 WTP，这是不合法的状态转换。

AC：　当 AC 的 Discovery 线程已经发送 Discovery Response，以便响应 Discovery Request 时，这个状态转换由该 Discovery 线程执行。

Discovery 到 Sulking (!)：当 AC Discovery 失败，这个转换在 WTP 上发生。

WTP：当 DiscoveryInterval 计时器到期并且 DiscoveryCount 变量等于 MaxDiscoveries 变量时，WTP 进入这个状态(参阅第 4-8 节)。一旦进入这个状态，WTP **必须**启动 SilentInterval 计时器。而在 Sulking 状态，**必须**忽略所有收到的 CAPWAP 协议消息。

AC：　对于 AC，这是不合法的状态转换。

Sulking 到 Idle (@)：当 WTP 必须重新开始 Discovery 阶段时，这个转换在 WTP 上发生。

WTP：当 SilentInterval 计时器(参阅第 4-7 节)到期，WTP 进入这个状态。FailedDTLSSessionCount、DiscoveryCount 和 FailedDTLSAuthFailCount 计数器都被重新设置为 0。

AC：　对于 AC，这是不合法的状态转换。

Sulking 到 Sulking (&)：Sulking 状态提供静默期，尽可能减小受到 Denial-of-Service (DoS) 攻击的可能。

WTP：忽略在 Sulking 状态期间从 AC 收到的所有分组。

AC：　对于 AC，这是不合法的状态转换。

Idle 到 DTLS Setup (3)：为了建立与对端的安全 DTLS 会话，这个转换发生。

WTP：通过调用 DTLSStart 指令，WTP 发起这个转换(参阅第 2-3-2-1 节)，这个转换启动与所选 AC 间建立 DTLS 会话，并且启动 WaitDTLS 计时器(参阅第 4-7 节)。如果 Discovery 阶段被旁路，那是假设 WTP 已在本地配置 ACs。

AC： 一旦从 Start 状态进入 Idle 状态，新创建的 Listener 线程自动转换到 DTLS Setup 并调用 DTLSListen 指令(参阅第 2-3-2-1 节)，然后启动 WaitDTLS 计时器(参阅第 4-7 节)。

Discovery 到 DTLS Setup (%)：为了建立与对端的安全 DTLS 会话，这个转换发生。

WTP：通过调用 DTLSStart 指令，WTP 发起这个转换(参阅第 2-3-2-1 节)，这个转换启动与所选 AC 间建立 DTLS 会话。连接到哪一个 AC 的决定是 Discovery 阶段的结果，在第 3-3 节介绍这方面内容。

AC： 对于 AC，这是不合法的状态转换。

DTLS Setup 到 Idle ($)：如果 DTLS 连接建立失败，这个转换发生。

WTP：当 WTP 从 DTLS 收到 DTLSEstablishFail 通知(参阅第 2-3-2-2 节)，以及 FailedDTLSSessionCount 或 FailedDTLSAuthFailCount 计数器没有达到 MaxFailedDTLSSessionRetry 变量的值(参阅第 4-8 节)，WTP 发起这个状态转换。这个出错通知终止安全 DTLS 会话建立。当收到这个通知时，FailedDTLSSessionCount 计数器增加。如果 WaitDTLS 计时器到期，这个状态转换也发生。

AC： 对于 AC，这是不合法的状态转换。

DTLS Setup 到 Sulking (*)：当反复尝试建立 DTLS 连接都失败时，这个转换发生。

WTP：当 FailedDTLSSessionCount 或 FailedDTLSAuthFailCount 计数器达到 MaxFailedDTLSSessionRetry 变量的值时，WTP 进入这个状态(参阅第 4-8 节)。一旦进入这个状态，WTP **必须**启动 SilentInterval 计时器。同时，在 Sulking 状态，**必须**忽略所有收到的 CAPWAP 协议消息和 DTLS 协议消息。

AC： 对于 AC，这是不合法的状态转换。

DTLS Setup 到 DTLS Setup (4)：当 DTLS Session 不能建立时，这个转换发生。

WTP：对于 WTP，这是不合法的状态转换。

AC： 当 AC 的 Listener 从 DTLS 收到 DTLSEstablishFail 通知时，AC 的 Listener 发起这个状态转换(参阅第 2-3-2-2 节)。这个出错通知终止安全 DTLS 会话建立。当收到这个通知时，增加 FailedDTLSSessionCount 计数器。接着，Listener 线程调用 DTLSListen 指令(参阅第 2-3-2-1 节)。

DTLS Setup 到 Authorize (5)：当输入的 DTLS 会话正在建立，并且为了着手会话建立 DTLS 栈需要授权时，这个转换发生。

WTP：当 WTP 收到 DTLSPeerAuthorize 通知时，这个状态转换发生(参阅第 2-3-2-2 节)。一旦进入这个状态，WTP 对照 AC 证书进行授权检查。关于 AC 授权的更多介绍参阅第 2-4-4 节。

AC： 当 DTLS 模块发起 DTLSPeerAuthorize 通知时，由 AC 的 Listener 线程处理这个状态转换(参阅第 2-3-2-2 节)。除了复制该状态的上下文以外，Listener 线程分支 Service 线程的实例。一旦生成，Service 线程对照 WTP 证书执行授权检查。关于 WTP 授权的更多介绍参阅第 2-4-4 节。

Authorize 到 DTLS Setup (6)：为了 Listener 线程能够侦听到新的输入会话，Listener 线程执行这个转换。

WTP：对于 WTP，这是不合法的状态转换。

AC： AC 的 Listener 线程创建 WTP 上下文和 Service 线程后，这个状态转换发生。接着 Listener 线程调用 DTLSListen 指令(参阅第 2-3-2-1 节)。

Authorize 到 DTLS Connect (a)：为了通知 DTLS 栈应当建立会话，这个转换发生。

WTP：WTP 成功授权 AC 的证书后，这个状态转换发生(参阅第 2-4-4 节)。这是通过调用 DTLSAccept DTLS 指令完成的(参阅第 2-3-2-1 节)。

AC： AC 成功授权 WTP 的证书后，这个状态转换发生(参阅第 2-4-4 节)。这是通过调用 DTLSAccept DTLS 指令完成的(参阅第 2-3-2-1 节)。

Authorize 到 DTLS Teardown (b)：为了通知 DTLS 栈应当终止会话，这个转换发生。

WTP：如果 WTP 无法使用 AC 证书授权 AC，这个状态转换发生。接着，WTP 通过调用 DTLSAbortSession 指令终止 DTLS 会话(参阅第 2-3-2-1 节)。如果 WaitDTLS 计时器到期，这个状态转换也会发生。WTP 启动 DTLSSessionDelete 计时器(参阅第 4-7-6 节)。

AC： 如果 AC 无法使用 WTP 证书授权 WTP，这个状态转换发生。接着，AC 通过调用 DTLSAbortSession 指令终止 DTLS 会话(参阅第 2-3-2-1 节)。如果 WaitDTLS 计时器到期，这个状态转换也会发生。AC 启动 DTLSSessionDelete 计时器(参阅第 4-7-6 节)。

DTLS Connect 到 DTLS Teardown (c)：当不能建立 DTLS Session 时，这个转换发生。

WTP：当 WTP 收到 DTLSAborted 或 DTLSAuthenticateFail 通知(参阅第 2-3-2-2 节)，指出不能成功建立 DTLS 会话时，这个状态转换发生。当由于 DTLSAuthenticateFail 通知导致这个转换发生时，增加 FailedDTLSAuthFailCount；否则，增加 FailedDTLSSessionCount 计数器。如果 WaitDTLS 计时器到期，这个状态转换也会发生。WTP 启动 DTLSSessionDelete 计时器(参阅第 4-7-6 节)。

AC： 当 AC 收到 DTLSAborted 或 DTLSAuthenticateFail 通知(参阅第 2-3-2-2 节)，指出不能成功建立 DTLS 会话，并且 FailedDTLSAuthFailCount 和 FailedDTLSSessionCount 计数器都还没有达到 MaxFailedDTLSSessionRetry 变量值时，这个状态转换发生(参阅第 4-8 节)。如果 WaitDTLS 计时器到期，这个状态转换也会发生。AC 启动 DTLSSessionDelete 计时器(参阅第 4-7-6 节)。

DTLS Connect 到 Join (d)：如果 DTLS Session 成功建立，这个转换发生。

WTP：当 WTP 收到 DTLSEstablished 通知(参阅第 2-3-2-2 节)，指出成功建立 DTLS 会话时，这个状态转换发生。当收到这个通知时，将 FailedDTLSSessionCount 计数器设置为 0。通过传送 Join Request 给 AC，WTP 进入 Join 状态。WTP 停止 WaitDTLS 计时器。

AC： 当 AC 收到 DTLSEstablished 通知(参阅第 2-3-2-2 节)，指出成功建立 DTLS 会话时，这个状态转换发生。当收到这个通知时，将 FailedDTLSSessionCount 计数器设置为 0。AC 停止 WaitDTLS 计时器，并启动 WaitJoin 计时器。

Join 到 DTLS Teardown (e)：如果加入过程失败，这个转换发生。

WTP：当 WTP 收到带有 Result Code 消息要素(该信息要素包含错误)的 Join Response 消息，或者如果由 AC 在 Join Response 消息中提供的 Image Identifier 不同于 WTP 目前运行的固件版本以及 WTP 在它的非易失性存储器中有要求的映像时，这个状态转换发生。这导致 WTP 启动 DTLSShutdown 指令(参阅第 2-3-2-1 节)。如果 WTP 收到下述 DTLS 通知之一，这个转换也会发生：

DTLSAborted、DTLSReassemblyFailure 或 DTLSPeerDisconnect。WTP 启动 DTLSSessionDelete 计时器(参阅第 4-7-6 节)。

AC： 如果 WaitJoin 计时器到期或者如果 AC 发送带有 Result Code 消息要素(该信息要

素包含错误)的 Join Response 消息，这个状态转换发生。这导致 AC 启动 DTLSShutdown 指令(参阅第 2-3-2-1 节)。如果 AC 收到下述 DTLS 通知之一，这个转换也会发生：

DTLSAborted、DTLSReassemblyFailure 或 DTLSPeerDisconnect。AC 启动 DTLSSessionDelete 计时器(参阅第 4-7-6 节)。

Join 到 Image Data (f)：WTP 和 AC 使用这个状态转换下载可执行的固件。

WTP：当 WTP 收到成功的 Join Response 消息并且确认在 Image Identifier 消息要素中的软件版本不同于它目前运行的映像的版本时，WTP 进入 Image Data 状态。WTP 也经过检测发现，要求的映像版本在 WTP 非易失性存储器中目前找不到(固件下载过程详细介绍参阅第 9-1 节)。WTP 启动 EchoInterval 计时器(参阅第 4-7 节)，并传送要求启动固件下载的 Image Data Request 消息(参阅第 9-1-1 节)。

AC：当 AC 从 WTP 收到 Image Data Request 消息，并发送它的 Join Response 给 WTP 后，这个状态转换发生。AC 停止 WaitJoin 计时器。AC **必须**传送 Image Data Response 消息(参阅第 9-1-2 节)给 WTP，该消息包括固件部分。

Join 到 Configure (g)：WTP 和 AC 使用这个状态转换交换配置信息。

WTP：当 WTP 收到成功的 Join Response 消息，并且确认包括的 Image Identifier 消息要素与它目前运行的映像相同，WTP 进入 Configure 状态。WTP 发送 Configuration Status Request 消息(参阅第 8-2 节)给 AC，该信息带有描述 WTP 目前配置的消息要素。

AC：当 AC 收到来自 WTP 的 Configuration Status Request 消息(参阅第 8-2 节)(该消息**可以**包括重写 WTP 配置的特定消息要素)时，这个状态转换发生。AC 停止 WaitJoin 计时器。AC 发送 Configuration Status Response 消息(参阅第 8-3 节)并启动 ChangeStatePendingTimer 计时器(参阅第 4-7 节)。

Configure 到 Reset (h)：这个状态转换用于重新设置连接，这样做的原因或者是由于配置阶段的错误，或者是 WTP 确认它需要重新设置以便让新配置生效。此 CAPWAP Reset 指令用于告诉对端，它将发起 DTLS 拆除。

WTP：当 WTP 收到指出错误的 Configuration Status Response 消息，或者当 WTP 确认由于新配置的特点需要重新设置 WTP 时，WTP 进入 Reset 状态。

AC：当 AC 收到来自 WTP 的 Change State Event 消息，该消息包括错误(由于该错误 AC 策略不允许 WTP 提供服务)时，AC 转换到 Reset 状态。当 AC 的 ChangeStatePendingTimer 计时器到期，这个状态转换也会发生。

Configure 到 DTLS Teardown (i)：当由于 DTLS 错误，配置过程终止时，这个转换发生。

WTP：当 WTP 收到下述 DTLS 通知之一时，它进入这个状态：DTLSAborted、DTLSReassemblyFailure 或 DTLSPeerDisconnect(参阅第 2-3-2-2 节)。如果频繁收到 DTLSDecapFailure 通知，WTP **可以**拆除 DTLS 会话。WTP 启动 DTLSSessionDelete 计时器(参阅第 4-7-6 节)。

AC：当 AC 收到下述 DTLS 通知之一时，它进入这个状态：DTLSAborted、DTLSReassemblyFailure 或 DTLSPeerDisconnect(参阅第 2-3-2-2 节)。如果 AC 频繁收到 DTLSDecapFailure 通知，它**可以**拆除 DTLS 会话。AC 启动 DTLSSessionDelete 计时器(参阅第 4-7-6 节)。

Image Data 到 Image Data (j)：由 WTP 和 ACS，在固件下载阶段使用 Image Data 状态。

WTP：当 WTP 收到指出 AC 有更多要发送的数据的 Image Data Response 消息时，WTP 进入 Image Data 状态。当 WTP 收到随后的多个 Image Data Requests 时，这个状态转换也会发生，每一次 WTP 都重新设置 ImageDataStartTimer 时间，以便确保

WTP 收到来自该 AC 的下一个预期的 Image Data Request。当 WTP 的 EchoInterval 计时器(参阅第 4-7-7 节)到期，这个状态转换也发生，在这种情况 WTP 发送 Echo Request 消息(参阅第 7-1 节)，并重新设置它的 EchoInterval 计时器。当 WTP 收到来自 AC 的 Echo Response 时，这个状态转换也会发生(参阅第 7-2 节)。

AC： 如果 AC 从 WTP(虽然已经在 Image Data 状态)收到 Image Data Response 消息，这个状态转换也会发生。当 AC 收到来自 WTP 的 Echo Request(参阅第 7-1 节)时，这个状态也会发生，在这种情况，AC 用 Echo Response 做出响应(参阅第 7-2 节)，并且重新设置它的 EchoInterval 计时器(参阅第 4-7-7 节)。

Image Data to Reset (k)：这个转换用于在映像下载后，重新启动 WTP 前，重新设置 DTLS 连接。

WTP：当映像下载完成，或如果 ImageDataStartTimer 计时器到期，WTP 进入 Reset 状态。一旦从 AC 收到指出失败的 Image Data Response 消息(参阅第 9-1-2 节)，WTP 也可以转换到这个状态。

AC： 当成功完成映像发送，或在映像下载处理期间发生错误，AC 进入 Reset 状态。

Image Data 到 DTLS Teardown (l)：当由于出现 DTLS 错误，终止固件下载处理时，这个转换发生。

WTP：当 WTP 收到下述 DTLS 通知之一时，WTP 进入这个状态：DTLSAborted、DTLSReassemblyFailure 或 DTLSPeerDisconnect(参阅第 2-3-2-2 节)。如果 WTP 频繁收到 DTLSDecapFailure 通知，WTP **可以**拆除 DTLS 会话。WTP 启动 DTLSSessionDelete 计时器(参阅第 4-7-6 节)。

AC：当 AC 收到下述 DTLS 通知之一时，AC 进入这个状态：DTLSAborted、DTLSReassemblyFailure 或 DTLSPeerDisconnect(参阅第 2-3-2-2 节)。如果 AC 频繁收到 DTLSDecapFailure 通知，AC **可以**拆除 DTLS 会话。AC 启动 DTLSSessionDelete 计时器(参阅第 4-7-6 节)。

Configure 到 Data Check (m)：当 WTP 和 AC 确认配置时，这个状态转换发生。

WTP：当 WTP 收到来自 AC 的成功 Configuration Status Response 消息时，WTP 进入这个状态。WTP 发送 Change State Event Request 消息(参阅第 8-6 节)。

AC： 当 AC 收到来自 WTP 的 Change State Event Request 消息(参阅第 8-6 节)时，这个状态转换发生。AC 用 Change State Event Response 消息(参阅第 8-7 节)响应。AC **必须**启动 DataCheckTimer 计时器，并停止 ChangeStatePendingTimer 计时器(参阅第 4-7 节)。

Data Check 到 DTLS Teardown (n)：当 WTP 没有完成 Data Check 交换时，这个转换发生。

WTP：如果 CAPWAP 重传超时发生前，WTP 没有收到 Change State Event Response 消息，这个状态转换发生。如果支撑可靠传输的 RetransmitCount 计数器达到 MaxRetransmit 变量(参阅第 4-7 节)，WTP 也转换到这个状态。WTP 启动 DTLSSessionDelete 计时器(参阅第 4-7-6 节)。

AC： 当 DataCheckTimer 计时器到期，AC 进入这个状态(参阅第 4-7 节)。AC 启动 DTLSSessionDelete 计时器(参阅第 4-7-6 节)。

Data Check 到 Run (o)：如果控制通道和数据通道间建立起连接，引起 WTP 和 AC 进入它们的正常运行状态，这个状态转换发生。

WTP：当 WTP 收到来自 AC 的成功 Change State Event Response 消息时，WTP 进入这个状态。WTP 初始化数据通道，这**可能**要求建立 DTLS 会话，启动 DataChannelKeepAlive 计时器(参阅第 4-7-2 节)，和发送 Data Channel Keep-Alive 分组(参阅第 4-4-1 节)。WTP 接着启动 EchoInterval 计时器和

DataChannelDeadInterval 计时器(参阅第 4-7 节)。

AC： 当 AC 收到 Data Channel Keep-Alive 分组(参阅第 4-4-1 节)，该分组带有 Session ID 消息要素，该消息要素匹配在 Join Request 消息中由 WTP 包括的消息要素时，这个状态转换发生。AC 关闭 DataCheckTimer 计时器。注意，如果 AC 策略要求加密数据通道，这个处理也要求建立数据通道 DTLS 会话。一旦收到 Data Channel Keep-Alive 分组，AC 发送它自己的 Data Channel Keep Alive 分组。

Run 到 DTLS Teardown (p)：如果在 DTLS 栈中发生错误，使得 DTLS 会话被拆除，这个状态转换发生。

WTP：当 WTP 收到下述 DTLS 通知之一时，WTP 进入这个状态：DTLSAborted、DTLSReassemblyFailure 或 DTLSPeerDisconnect(参阅第 2-3-2-2 节)。如果 WTP 频繁收到 DTLSDecapFailure 通知，WTP **可以**拆除 DTLS 会话。如果支撑可靠传输的 RetransmitCount 计数器达到 MaxRetransmit 变量(参阅第 4-7 节)，WTP 也转换到这个状态。WTP 启动 DTLSSessionDelete 计时器(参阅第 4-7-6 节)。

AC： 当 AC 收到下述 DTLS 通知之一时，AC 进入这个状态：DTLSAborted、DTLSReassemblyFailure 或 DTLSPeerDisconnect(参阅第 2-3-2-2 节)。如果 AC 频繁收到 DTLSDecapFailure 通知，AC **可以**拆除 DTLS 会话。如果支撑可靠传输的 RetransmitCount 计数器达到 MaxRetransmit 变量(参阅第 4-7 节)，AC 转换到这个状态。如果 AC 的 EchoInterval 计时器(参阅第 4-7-7 节)到期，这个转换也发生。AC 启动 DTLSSessionDelete 计时器(参阅第 4-7-6 节)。

Run 到 Run (q)：这是正常运行状态。

WTP：这是 WTP 的正常运行状态。只要 WTP 发送请求给 AC，WTP 就重新设置它的 EchoInterval 计时器。有许多事件会导致这个状态转换发生：

Configuration Update：WTP 收到 Configuration Update Request 消息(参阅第 8-4 节)。WTP **必须**用 Configuration Update Response 消息(参阅第 8-5 节)响应。

Change State Event：WTP 收到 Change State Event Response 消息，或者 WTP 确定它必须发起 Change State Event Request 消息，作为在无线电设备状态中出现故障或改变的结果。

Echo Request：WTP 发送 Echo Request 消息(参阅第 7-1 节)或从 AC 收到相应的 Echo Response 消息(参阅第 7-2 节)。当 WTP 收到 Echo Response 时，WTP 重新设置它的 EchoInterval 计时器(参阅第 4-7-7 节)。

Clear Config Request：WTP 收到 Clear Configuration Request 消息(参阅第 8-8 节)，并且 WTP **必须**生成相应的 Clear Configuration Response 消息(参阅第 8-9 节)。WTP **必须**将它的配置重新恢复到厂家默认值。

WTP Event：WTP 发送 WTP Event Request 消息，传送信息给 AC(参阅第 9-4 节)。WTP 从 AC 收到 WTP Event Response 消息(参阅第 9-5 节)。

Data Transfer：WTP 发送 Data Transfer Request 或 Data Transfer Response 消息给 AC(参阅第 9-6 节)。WTP 收到来自 AC 的 Data Transfer Request 或 Data Transfer Response 消息(参阅第 9-6 节)。一旦收到 Data Transfer Request，WTP 发送 Data Transfer Response 给 AC。

Station Configuration Request：WTP 收到 Station Configuration Request 消息(参阅第 10-1 节)，对于这个消息，WTP **必须**用 Station Configuration Response 消息响应(参阅第 10-2 节)。

AC： 这是 AC 的正常运行状态。注意，接收来自 WTP 的任何 Request 会引起 AC 重新设置它的 EchoInterval 计时器(参阅第 4-7-7 节)。

Configuration Update：AC 发送 Configuration Update Request 消息(参阅第 8-4 节)给 WTP，以便更新 WTP 的配置。AC 接收来自 WTP 的 Configuration Update Response 消息(参阅第 8-5 节)。

Change State Event：AC 接收 Change State Event Request 消息(参阅第 8-6 节)，对于这个消息，AC **必须**用 Change State Event Response 消息响应(参阅第 8-7 节)。

Echo Request：AC 接收 Echo Request 消息(参阅第 7-1 节)，对于这个消息 AC **必须**用 Echo Response 消息响应(参阅第 7-2 节)。

Clear Config Response：AC 发送 Clear Configuration Request 消息(参阅第 8-8 节)给 WTP，以便清除 WTP 的配置。AC 接收来自 WTP 的 Clear Configuration Response 消息(参阅第 8-9 节)。

WTP Event：AC 从 WTP 接收 WTP Event Request 消息(参阅第 9-4 节)，AC **必须**生成相应的 WTP Event Response 消息(参阅第 9-5 节)。

Data Transfer：AC 发送 Data Transfer Request 或 Data Transfer Response 消息给 WTP(参阅第 9-6)。AC 接收来自 WTP 的 Data Transfer Request 或 Data Transfer Response 消息(参阅第 9-6 节)。一旦收到 Data Transfer Request，AC 发送 Data Transfer Response 给 WTP。

Station Configuration Request：AC 发送 Station Configuration Request 消息(参阅第 10-1 节)或从 WTP 接收相应的 Station Configuration Response 消息(参阅第 10-2 节)。

Run 到 Reset (r)：当或者 AC 或者 WTP 拆除连接时，使用这个状态转换。发生此可能是正常操作的一部分，也可能是由于错误条件引起。

WTP：当 WTP 收到来自 AC 的 Reset Request 消息时，WTP 进入 Reset 状态。

AC：当 AC 发送 Reset Request 消息给 WTP 时，AC 进入 Reset 状态。

Reset 到 DTLS Teardown (s)：当完成 CAPWAP 重新设置，终止 DTLS 会话时，这个转换发生。

WTP：当 WTP 发送 Reset Response 消息时，这个状态转换发生。WTP 不调用 DTLSShutdown 指令(参阅第 2-3-2-1 节)。WTP 启动 DTLSSessionDelete 计时器(参阅第 4-7-6 节)。

AC：当 AC 收到 Reset Response 消息时，这个状态转换发生。这引起 AC 发起 DTLSShutdown 指令(参阅第 2-3-2-1 节)。AC 启动 DTLSSessionDelete 计时器(参阅第 4-7-6 节)。

DTLS Teardown 到 Idle (t)：如果关闭 DTLS 会话，这个转换发生。

WTP：当 WTP 成功清理与控制平面 DTLS 会话有关的所有资源，或者如果 DTLSSessionDelete 计时器(参阅第 4-7-6 节)到期时，这个状态转换发生。如果 DTLS 会话是为数据平面建立的，也关闭数据平面 DTLS 会话，释放所有资源。为状态机当前实例设置的任何计时器也将清除。

AC：对于 AC，这是不合法的状态转换。

DTLS Teardown 到 Sulking (u)：如果反复尝试建立 DTLS 连接失败，这个转换发生。

WTP：当 FailedDTLSSessionCount 或 FailedDTLSAuthFailCount 计数器达到 MaxFailedDTLSSessionRetry 变量值时，WTP 进入这个状态(参阅第 4-8 节)。一旦进入这个状态，WTP **必须**启动 SilentInterval 计时器。而在 Sulking 状态，**必须**忽略所有收到的 CAPWAP 协议消息和 DTLS 协议消息。

AC：对于 AC，这是不合法的状态转换。

DTLS Teardown 到 Dead (w)：如果 DTLS 会话关闭，这个转换发生。

WTP：对于 WTP，这是不合法的状态转换。

AC：当 AC 成功清除与控制平面 DTLS 会话相关的所有资源，或者如果 DTLSSessionDelete 计时器(参阅第 4-7-6 节)到期时，这个状态转换发生。如果 DTLS 会话是为数据平面建立的，数据平面 DTLS 会话也关闭，并释放所有资源。为目前的状态机实例建立的任何计时器也将清除。终止 AC 的 Service 线程。

2-3-2 CAPWAP/DTLS 接口

本节介绍由 CAPWAP 使用的 DTLS Commands，以及收到的、从 DTLS 到 CAPWAP 协议栈的通知。

2-3-2-1 CAPWAP 到 DTLS 的指令

为 CAPWAP 到 DTLS API 定义了 6 条指令。这些“指令”是概念性的，可以作为一个或多个功能调用实现。提供这个 API 定义，是为了澄清集成 CAPWAP 状态机的 DTLS 分量和 CAPWAP 分量间的互动。

下面是一组最低限度需要的指令应用程序编程接口(APIs)：

- 发送 DTLSStart 到 DTLS 分量，引起 DTLS 会话建立。一旦调用 DTLSStart 指令，启动 WaitDTLS 计时器。因为 AC 不发起 DTLS 会话，WTP 发起这个 DTLS 指令。
- 发送 DTLSListen 到 DTLS 分量，使 DTLS 分量能够监听到达的 DTLS 会话请求。
- 发送 DTLSAccept 到 DTLS 分量，使 DTLS 会话建立能够成功继续。
- 发送 DTLSAbortSession 到 DTLS 分量，诱发终止正在建立过程中的会话。当 WaitDTLS 计时器到期，也发送这个指令。如果执行这个指令，FailedDTLSSessionCount 计数器增加。
- 发送 DTLSShutdown 到 DTLS 分量，引起会话拆除。
- DTLSMtuUpdate 由 CAPWAP 分量发送，以便修改由 DTLS 分量使用的 MTU 长度。关于 MTU Discovery 的更多介绍参阅第 3-5 节。默认长度是 1468 bytes。

2-3-2-2 DTLS 到 CAPWAP 的通知

为 DTLS 到 CAPWAP API 定义了多个 DTLS 通知。这些“通知”是概念上的，可以用多种方式实现(例如，作为函数返回值)。提供这个 API 定义，是为了澄清集成的 CAPWAP 状态机的 DTLS 分量和 CAPWAP 分量间的互动。重要的是要注意到，下面列出的通知**可以**引起 CAPWAP 状态机，使用没有在第 2-3-1 节列出的状态转换，从一个状态跳到另一个状态。当下面列出的通知发生时，在图 4 中显示的目标 CAPWAP 状态变成当前状态。

下面是 API 通知列表：

- 在 DTLS 会话建立期间，一旦收到对端的身份，发送 DTLSPeerAuthorize 到 CAPWAP 分量。这个通知可由 CAPWAP 分量根据对端身份，用于认证会话。认证处理将导致 CAPWAP 分量发起 DTLSAccept 指令或 DTLSAbortSession 指令。
- 发送 DTLSEstablished 到 CAPWAP 分量，指出现在有安全通道，使用在 DTLS 初始化处理期间提供的参数。当收到这个通知时，设置 FailedDTLSSessionCount 计数器为 0。当收到这个通知时， WaitDTLS 计时器停止。
- 当 DTLS 会话建立失败(或者是由于本地错误，或者是由于对端反对建立会话)时，发送 DTLSEstablishFail。当收到这个通知时，FailedDTLSSessionCount 计数器增加。
- 当由于授权错误造成 TDLS 会话建立失败时，发送 DTLSAuthenticateFail。当收到这个通知时，FailedDTLSAuthFailCount 计数器增加。
- 发送 DTLSAborted 到 CAPWAP 分量，指出会话终止完成(按照 CAPWAP 要求)；发生此，

证实 DTLS 会话终止或 WaitDTLS 计时器到期。当收到这个通知时，WaitDTLS 计时器停止。

- 为了指出 DTLS 分段重组失败，**可以**发送 DTLSReassemblyFailure 给 CAPWAP 分量。
- 为了指出解封装失败，**可以**发送 DTLSDecapFailure 给 CAPWAP 模块。为了指出加密/认证失败，**可以**发送 DTLSDecapFailure 给 CAPWAP 模块。这个通知仅用于提供信息，不打算在 CAPWAP 状态机中引起改变(参阅第 12-4 节)。
- 为了指出已经拆除 DTLS 会话，发送 DTLSPeerDisconnect 给 CAPWAP 分量。注意，仅当 DTLS 会话已经建立时，才接收这个通知。

2-4 在 CAPWAP 协议中使用 DTLS

DTLS 与 CAPWAP 协议紧密集成，是后者的安全包裹者。在本文档中，把 DTLS 和 CAPWAP 作为名义上不同的实体分开讨论；然而，它们结合非常紧密，实施起来甚至难以分割。因为当前有 DTLS 库实现可用，以及因为在广泛应用的加速硬件中常常使用安全协议(例如，IPsec，TLS)，在本文档中维持一个标准化的差别既方便又具有前瞻性。

这一节介绍 DTLS 模块和 CAPWAP 模块在正常操作过程中相遇时，通过“指令”(CAPWAP 到 DTLS)和“通知”(DTLS 到 CAPWAP)，实现相互间互动的细节。

2-4-1 DTLS 握手处理流程

DTLS 握手处理的详细介绍参见[RFC4347]。这一节介绍 DTLS 会话建立流程和 CAPWAP 协议间的互动。注意，下面显示的概念性 DTLS 状态用于帮助理解 DTLS 状态转换的点。正常情况，DTLS 握手流程如图 5 所示。(**注意**：这个举例使用证书，但是也支持预共享密钥。)

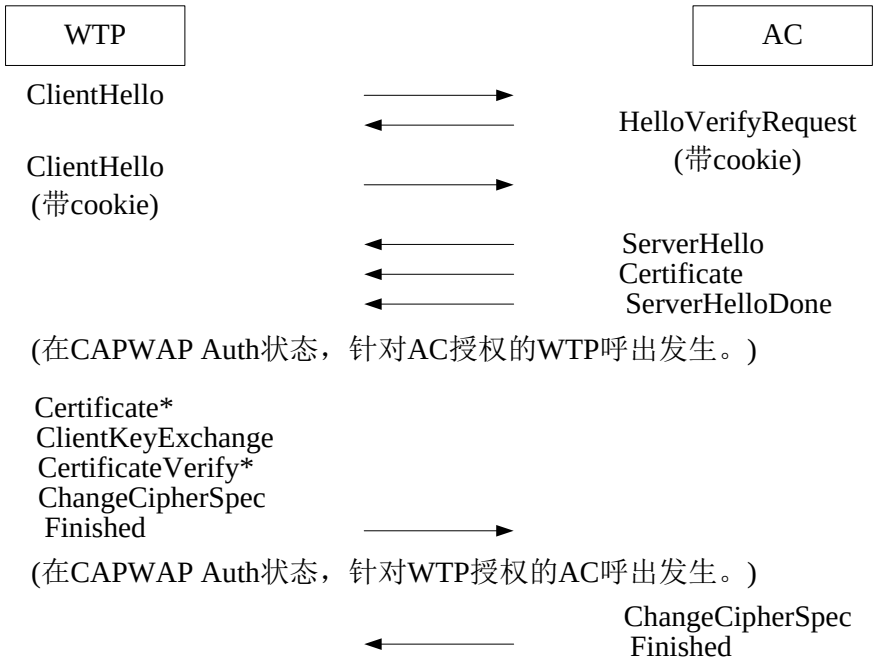


图 5 DTLS 握手

DTLS，如规定的，提供它自己的带指数回退(back-off)的重传计时器。[RFC4347]没有规定重传应当持续多长时间。因此，超时的不完整 DTLS 握手完全是 CAPWAP 模块的责任。

CAPWAP 使用的 DTLS 实现**必须**支持 TLS Session Resumption。会话恢复一般用于建立数据通道使用的 DTLS 会话。因为数据通道使用不同于控制通道的端口号，在 WTP 上的 DTLS 实现**必须**提供接口，该接口使 CAPWAP 模块能够请求会话恢复，尽管使用不同的端口号(TLS 实现通常仅当连接到相同 IP 地址和端口号时尝试会话恢复)。注意，不保证会话恢复发生，相反，可能出现整个 DTLS 握手。

CAPWAP 使用的 DTLS 实现**必须**按[RFC4347]第 3-3 节规定，使用重放检测。因为 CAPWAP 协议通过重新加密丢失的帧，处理重传，应当静默抛弃任何(无意或故意的)重复 DTLS 帧。

2-4-2 DTLS 会话建立

WTP，或者通过 Discovery 流程或者通过预配置，决定连接到哪一个 AC。WTP 使用 DTLSStart 指令请求与所选 AC 建立安全连接。在发起 DTLS 握手前，WTP 将 WaitDTLS 计时器置 1。一旦调用 DTLSStart 指令或 DTLSListen 指令，WTP 和 AC 分别将 WaitDTLS 计时器置 1。如果计时器到期前没有收到 DTLSEstablished 通知，通过发布 DTLSAbortSession DTLS 指令终止 DTLS 会话。这个通知引起 CAPWAP 模块转换到 Idle 状态。一旦收到 DTLSEstablished 通知，WaitDTLS 计时器关闭。

2-4-3 DTLS 错误处理

如果 AC 或 WTP 不响应它的对端发出的任何 DTLS 握手消息，TDLS 规范要求重传该消息。注意，在握手期间，当 AC 和 WTP 盼望补充的握手消息，而盼望的消息没有收到，它们都将重传(注意，CAPWAP Control 消息采用不同方式重传：所有 CAPWAP Control 消息或者是请求或者是响应，发送请求的对端负责重传)。

如果经过重传 WTP 或 AC 仍然没有收到盼望的 DTLS 握手消息，WaitDTLS 计时器终将到期，会话将被终止。如果对端间的通信完全失败，或者如果对端中的一方发送 DTLS Alert 消息，该消息在传输中丢失(DTLS 不重传 Alert 消息)，都会发生会话终止。

如果 cookie 无法通过验证，这可能表示发生 WTP 错误，或者表示可能遭遇 DoS 攻击。因此，**应当**尽量减小 AC 资源利用。AC **可以**记录指出故障的消息，**应当**将该消息看作是好像没有 cookie 存在。

因为 DTLS Handshake 消息可能大于最大记录长度，DTLS 支持跨多个记录分段 Handshake 消息。有几个造成重组错误的潜在原因，包括重叠和/或分段丢失。TDLS 分量**必须**发送 DTLSReassemblyFailure 通知给 CAPWAP 分量。是否与通知一起给出精确信息是实施问题，因此这个文档不作讨论。一旦收到这类错误，CAPWAP 分量**应当**记录相应错误消息。是继续完成流程还是终结 DTLS 会话取决于具体实施。

DTLS 解封装错误有 3 类：解密错误、认证错误和畸形的 DTLS 记录首部。因为 DTLS 在封装前认证数据，如果解密失败，不首先尝试认证分组是难以检测到此的。如果认证失败，也极有可能是因为解密错误，但不能保证。不尝试推出(并要求执行)检测解密失败的算法，解密失败被作为认证失败报告。当这类错误发生时，DTLS 分量**必须**提供 DTLSDecapFailure 通知给 CAPWAP 分量。如果检测到畸形的 DTLS 记录首部，**应当**静默抛弃该分组，并且接收方**可以**记录错误消息。

目前仅定义了一种封装错误：MTU 过大。作为 DTLS 会话建立的一部分，CAPWAP 分量通知 DTLS 分量 MTU 大小。当 CAPWAP 分量发送 DTLSMtuUpdate 指令给 DTLS 分量时，可以随时修改 MTU 大小(参阅第 2-3-2-1 节)。提供给 DTLS 栈的值是 MTU Discovery 流程的结果，在第 3-5 节介绍此。只要发送请求将产生超过此 MTU 的分组，DTLS 分量返回这个通知给 CAPWAP 分量。

2-4-4 DTLS 端点认证和授权

DTLS 支持采用证书或预共享密钥的端点认证。适合每种端点认证方法的 TLS 算法套件如下。

2-4-4-1 采用证书认证

CAPWAP 实现仅使用推荐与 DTLS 一起使用的密码套件，参阅[DTLS-DESIGN]。目前，如果 CAPWAP 认证使用证书，**必须**支持下述算法：

- TLS_RSA_WITH_AES_128_CBC_SHA [RFC5246]

如果使用证书，**应当**支持下述算法：

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA [RFC5246]

如果使用证书，**可以**支持下述算法：

- TLS_RSA_WITH_AES_256_CBC_SHA [RFC5246]
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA [RFC5246]

在将来的 CAPWAP 规范中**可以**定义补充密码。

2-4-4-2 使用预共享密钥认证

从安全角度看，预共享密钥(Pre-Shared Key, PSK)面临重大挑战，考虑到此原因，它们的使用不容乐观。在[RFC4279]中定义了几种采用预共享密钥的认证方法，我们关注下面两个：

- 预共享密钥密钥交换算法---最简单方法，密码套件仅使用对称密钥算法。
- DHE_PSK 密钥交换算法---使用 PSK 来授权 Diffie-Hellman 交换。这些密码套件提供一些防范字典攻击的额外保护，也提供完善前向保密(Perfect Forward Secrecy, PFS)。

第一种方法(明文 PSK)容易受到被动字典攻击；因此，尽管**必须**支持这个算法，如果选择该方法应采取特别关照。尤其是**不应当**使用用户可读的密码，应强烈反对使用短 PSKs。

当使用预共享密钥时，**必须**支持下述加密算法：

- TLS_PSK_WITH_AES_128_CBC_SHA [RFC5246]
- TLS_DHE_PSK_WITH_AES_128_CBC_SHA [RFC5246]

当使用预共享密钥时，**可以**支持下述算法：

- TLS_PSK_WITH_AES_256_CBC_SHA [RFC5246]
- TLS_DHE_PSK_WITH_AES_256_CBC_SHA [RFC5246]

在后续 CAPWAP 规范中**可以**定义补充密码。

2-4-4-3 证书应用

要求由 AC 和 WTP 授权证书，以便只有 AC 可以行使 AC 功能，只有 WTP 可以行使 WTP 功能。对 AC 或 WTP 的这个功能限制，要求 AC 使用的证书**必须**不同于 WTP 使用的证书。为了实现这个区别，x.509 证书**必须**包括 Extended Key Usage(EKU)证书扩展[RFC5280]。

EKU 字段指出一个或多个可以应用证书的场合。EKU 字段是授权的基础部分。在[RFC5280]和[ISO.9834-1.1993]中描述的 EKU 字段句法如下：

```
ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId
KeyPurposeId ::= OBJECT IDENTIFIER
```

这里，我们定义两个 KeyPurposeId 值，一个用于 WTP，一个用于 AC。包括这两个值中的一个表示证书被分别授权由 WTP 或 AC 使用。这两个值被格式化为 id-kp 字段。

id-kp OBJECT IDENTIFIER ::=
{ iso(1) identified-organization(3) dod(6) internet(1)
security(5) mechanisms(5) pkix(7) 3 }
id-kp-capwapAC OBJECT IDENTIFIER ::= { id-kp 18 }
id-kp-capwapWTP OBJECT IDENTIFIER ::= { id-kp 19 }

所有 ACPWAP 设备**必须**支持 ExtendedKeyUsage 证书扩展，如果该扩展存在于证书中。如果该扩展存在，那么证书**必须**或者有 id-kp-capwapAC，或者有 id-kp-anyExtendedKeyUsage，keyPurposeID 充当 AC。

类似，如果该扩展存在，设备必须有 id-kpcapwapWTP，或者有 id-kp-anyExtendedKeyUsage，keyPurposeID 充当 WTP。

CAPWAP 证书合法性检验过程的一部分包括，确保包括适当的 EKU，以及仅当该扩展适当代表该设备时才允许建立 CAPWAP 会话。例如，AC **不应当**接受来自另一个 AC 的连接请求，因此**必须**验证在证书中有 id-kp-capwapWTP EKU。

CAPWAP 实现**必须**支持 WTP 和 AC 的公用名(common name, CN)是那台设备的 MAC 地址的证书。MAC 地址**必须**用 PrintableString 格式编码，使用公认的 01:23:45:67:89:ab MAC 地址格式。CN 字段**可以**包括 EUI-48 [EUI-48] 或 EUI-64 [EUI-64] MAC Address 格式中的任何一个。与依据生产制造期间提供的设备证书的其他标准(诸如，Packet Cable [PacketCable]、Cable Labs [CableLabs]和 WiMAX [WiMAX])相比，这看似非常规使用的 CN 字段其实是异曲同工。关于 CN 字段中 MAC 地址使用的更多介绍参阅第 12-8 节。

ACs 和 WTPs **必须**授权(例如，通过访问控制列表)它们正在连接设备的证书，例如，根据发行人、MAC 地址，或证书中规定的组织信息。证书中规定的身份绑定特定 DTLS 会话到指定的一对相互认证和授权的 MAC 地址。特定授权过滤器结构，在大多数情况，是实现细节，不属于本规范讨论范围。然而，最低限度，所有设备**必须**验证已按照对端设备角色(AC 对应 WTP)设置相应的 EKU 位，并且证书发行人与讨论的域相称。

2-4-4-4 PSK 应用

如果 DTLS 使用 PSK Ciphersuites，ServerKeyExchange 消息**必须**包括“PSK 身份提示”字段，ClientKeyExchange 消息**必须**包括“PSK 身份”字段。这些字段用于帮助 WTP 选择适合与 AC 一起使用的 PSK，接着告诉 AC 正在使用哪一个密钥。当向 WTPs 和 ACs 提供 PSKs 时，**必须**规定密钥的 PSK Hint 和 PSK Identity。

PSK Hint **应当**唯一标识 AC，PSK Identity **应当**唯一标识 WTP。**建议**这些提示和身份采用各自设备的 ASCII HEX 格式 MAC 地址，因为每个 WTP 和 AC 的两两组合**应当**有唯一的 PSK。PSK Hint 和 Identity **应当**足以执行授权，因为简单拥有 PSK 知识不必然暗示授权。

如果在 CAPWAP 网络上多个设备使用单个 PSK，**不推荐**这样做，PSK Hint 和 Identity 可能不再是 MAC 地址，所以**应当**选择适当提示和身份来标识一组应用 PSK 的设备。

第 3 章 CAPWAP 传送

使用标准 UDP 客户端/服务器模式建立 WTP 和 AC 间的通信。CAPWAP 协议支持 UDP 和 UDP-Lite[RFC3828]传输协议。当在 IPv4 上运行时，CAPWAP Control 和 Data 通道使用 UDP。

当在 IPv6 上运行时，CAPWAP Control 通道总是使用 UDP，而 CAPWAP Data 通道可以使用 UDP 或 UDP-Lite。UDP-Lite 是 CAPWAP Data 通道的默认传输协议。然而，如果发现中间件(middlebox)或 IPv4 到 IPv6 网关，CAPWAP Data 通道使用 UDP。

这一章介绍如何在 IP 和 UDP/UDP-Lite 传输协议上携带 CAPWAP 协议。CAPWAP

Transport Protocol 消息要素，第 4-6-14 节，介绍在决定使用哪一个传输协议的过程中使用的规则。

为使 CAPWAP 兼容网络中可能的中间件，CAPWAP 实现**必须**在与它们从给定对端接收流量的相同端口上发送返回流量。此外，由 CAPWAP 节点生成的任何不请自来的请求**必须**在同一端口上发送。

3-1 UDP 传送

CAPWAP 协议的其中一个要求是允许 WTP 驻留在中间件、防火墙和/或 Network Address Translation (NAT)设备后面。因为 WTP(客户端)发起到 AC(服务器)众所周知 UDP 端口的 CAPWAP 会话，使用 UDP 是合乎逻辑的选择。当 CAPWAP 在 IPv4 上运行时，**必须**将 CAPWAP 分组中的 UDP 校验和字段设置为 0。

如第 1-4 节定义的，从 WTP 发送到 AC 的 CAPWAP 协议控制分组使用 CAPWAP Control 通道。在 AC 中的 CAPWAP 控制端口是众所周知的 UDP 端口 5246。在 WTP 中的 CAPWAP 控制端口可以是由 WTP 选择的任何端口。

如第 1-4 节定义的，从 WTP 发送到 AC 的 CAPWAP 协议数据分组使用 CAPWAP Data 通道。在 AC 中的 CAPWAP 数据端口是众所周知的 UDP 端口 5247。如果 AC 准许管理员改变 CAPWAP 控制端口，CAPWAP 数据端口**必须**是下一个连续的端口号。在 WTP 中的 CAPWAP 数据端口可以是由 WTP 选择的任何端口。

3-2 UDP-Lite 传送

当在 IPv6 上运行 CAPWAP 时，UDP-Lite 是默认的传输协议，它去掉了对每个分组要求的校验和处理(与 IPv6 上 UDP 应用[RFC2460]相比)。如果使用 UDP-Lite，校验和字段**必须**选择 8 [RFC3828]。

UDP-Lite 使用与 UDP 相同的端口分配。

3-3 AC 发现

AC Discovery 阶段使 WTP 能够确定哪些 ACs 可用，能够让 WTP 选择与自己建立 CAPWAP 会话的最佳 AC。当 WTP 进入可选的 Discovery 状态，Discovery 阶段发生。如果 WTP 使用预先配置的 AC，它不需要完成 AC Discovery 阶段。这一节详细介绍 WTP 动态发现候选 ACs 使用的机制。

WTP 和 AC 经常不驻留在相同的 IP 子网(广播域)。如处于这种情况，WTP 必须能够在不要求网络开启多播业务条件下，发现 AC。

当 WTP 尝试与 AC 建立通信时，它发送 Discovery Request 消息并接收来自 AC(s)的 Discovery Response 消息。WTP **必须**将 Discovery Request 消息发送到：或者是限定的广播 IP 地址(255.255.255.255)，众所周知的 CAPWAP 多播地址(224.0.1.140)，或者是该 AC 的单播 IP 地址。对于 IPv6 网络，因为不使用广播，用“所有 ACs 多播地址”(FF0X:0:0:0:0: 0:0:18C)取而代之。一旦收到 Discovery Request 消息，无论 Discovery Request 消息是作为广播、多播还是单播消息发送的，AC 发送 Discovery Response 消息到该 WTP 的单播 IP 地址。

WTP 使用限定的 IP 广播、多播或单播 IP 地址，根据实现需要而定。另一方面，ACs **必须**支持广播、多播和单播发现。

当 WTP 发送 Discovery Request 消息到单播地址时，WTP 必须首先获得该 AC 的该 IP 地址。在 WTP 非易失性存储器上 AC IP 地址的任何静态配置根据实现需要确定。然而，可以补充动态方案，例如：

DHCP：关于用 DHCP 发现 AC IP 地址的更多介绍参阅[RFC5417]。

DNS： WTP **可以**支持使用 DNS Service Records (SRVs) [RFC2782]发现 AC 地址。在这种情况，WTP 首先获得(例如，从本地配置)正确的域名前缀(例如，“example.com”)，以及用 Service 名称“capwap-control”和 Proto“udp”执行 SRV 查询。于是，在 DNS 中解析的名称将是，例如，“_capwapcontrol._ udp.example.com”。注意，SRV 记录**可以**规定控制通道的非默认端口号；数据通道的端口号是下一个端口号(控制通道端口+1)。

AC 也**可以**在 Discovery Response 消息中，通过 AC IPv4 List (参阅第 4-6-2 节)和 AC IPv6 List(参阅第 4-6-2 节)传递替代 ACs 给 WTP。在这两个消息要素中提供地址，是打算除以上列出方法外，通过其他方法帮助 WTP 发现额外的 ACs。

带有 Priority 消息要素的 AC Name (参阅第 4-6-5 节)用于传递一系列优先的 ACs 给 WTP。WTP **应当**尝试使用由该 AC 提供的排序中列出的 ACs。通过 Discovery 消息交换处理 Name-to-IP Address 映射，这其中 ACs 在 Discovery Response 消息中，以 AC Name(参阅第 4-6-4 节)消息要素，提供它们(即 ACs)的身份。

一旦WTP从候选ACs收到Discovery Response消息，WTP**可以**使用其他因素确定优先的 AC。例如，每个绑定限定WTP Radio Information消息要素(参阅第2-1节)，AC在Discovery Response 消息中包括该消息要素。带有一个或多个这样的消息要素是为了识别由该 AC 支持的 CAPWAP 绑定。WTP 可以根据通告中支持的绑定连接到 AC。

3-4 分段/重组

尽管 IP 提供分段和重组业务，CAPWAP 协议也提供这类业务。使用 CAPWAP 协议的环境包括防火墙设备、NAT 设备和“中间件”设备，为了尽量减小受到 DoS 攻击的可能，这些设备倾向于丢弃 IP 分段。通过在应用层提供分段和重组，由于隧道化 CAPWAP 协议分量，任何要求的分段变得对这些中继设备透明。因此，CAPWAP 协议可以在任何网络拓扑(包括防火墙设备、NAT 设备和中间件设备)中使用。

重要的是要注意到，CAPWAP 使用的分段机制有已知的局限性和不足，其类似于在[RFC4963]中描述的情况。Fragment ID 字段(参阅第 4-3 节)的有限大小可能引起该字段重叠，进而引起将来自不同数据报的分段不正确拼接在一起(称作“错误关联”)。例如，采用 1500 MTU 的 100Mphs 链路(引起在 1450 字节分段)会导致持续 8 秒时间的 Fragment ID 字段重叠。因此，CAPWAP 实施者应根据预期无线技术的吞吐量，适当估算用于重组的缓存器的大小。

CAPWAP 实现**应当**执行 MTU Discovery(参阅第 3-5 节)，这样可以避免分段需要。在撰写本规范时，绝大多数企业的交换和路由基础设施能够支持“小巨型(mini-jumbo)”帧(1800 字节)，这排除了分段需要(假设台站的 MTU 是 1500 字节)。当 WTP 与 AC 经广域网(Wide Area Network, WAN)通信时一般仍需要分段。因此， CAPWAP 协议的将来版本**应当**考虑或者增加 Fragment ID 字段的大小，或者提供替代扩展。

3-5 MTU 发现

一旦 WTP 发现它希望与之建立 CAPWAP 会话的 AC，WTP **应当**执行 Path MTU (PMTU)发现。执行 PMTU 发现的一种推荐方法是让 WTP 发送 Discovery Request(参阅第 5-1 节)消息，并且包括 MTU Discovery Padding 消息要素(参阅第 4-6-32 节)。用于 PMTU 发现的实际步骤，针对 IPv4 的在[RFC1191]中介绍；针对 IPv6 的**应当**使用[RFC1981]中介绍的方法。另一方面，实施者**可以**使用[RFC4821]中定义的步骤。WTP 也**应当**使用这两个 RFCs 中提供的指南，使用伴随 MTU Discovery Padding 消息要素(参阅第 4-6-32 节)的 Primary Discovery Request(参阅第 5-3 节)，定期重新评估 PMTU。当 MTU 最初是已知的，或在现有会话已经存在情况下 MTU 被更新，将发现的 PMTU 用于配置 DTLS 分量(参阅第 2-3-2-1 节)，而非

DTLS 帧需要被分段以适应该 MTU，如第 3-4 节中定义的。

第 4 章　CAPWAP 分组格式

这一章包含 CAPWAP 协议分组格式。CAPWAP 协议分组由一个或多个 CAPWAP Transport Layer 分组首部，再加上 CAPWAP 消息组成。CAPWAP 消息可以是 Control 类型或 Data 类型，Control 分组携带信令，Data 分组携带用户净荷。CAPWAP Data 分组的 CAPWAP 帧格式，以及封装 CAPWAP Data 分组和 Control 分组的 DTLS 的 CAPWAP 帧格式在下面定义。

CAPWAP Control 协议包括两条完全没有 DTLS 保护的消息：Discovery Request 消息和 Discovery Response 消息。这些消息需要无阻碍地让 CAPWAP 协议适当识别和处理它们。CAPWAP 协议分组格式如附图 1 所示。

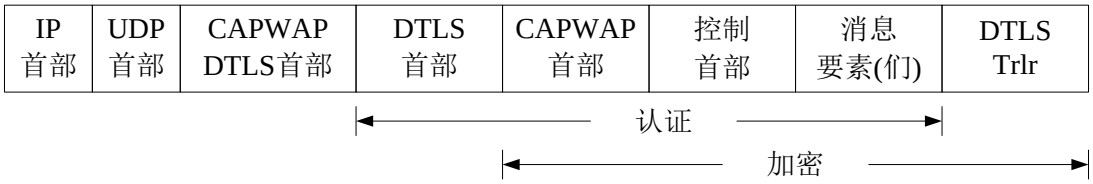
CAPWAP Control Packet (Discovery Request/Response)格式:

IP 首部	UDP 首部	CAPWAP 首部	控制 首部	消息 要素(们)

附图 1　CAPWAP Control Packet (Discovery Request/Response)格式

必须通过 DTLS 协议保护所有其他 CAPWAP Control 协议消息，这确保认证和加密这些分组。这些分组包括 CAPWAP DTLS Header，该首部在第 4-2 节介绍。这些分组的格式如附图 2 所示。

CAPWAP Control Packet (DTLS Security Required)格式:



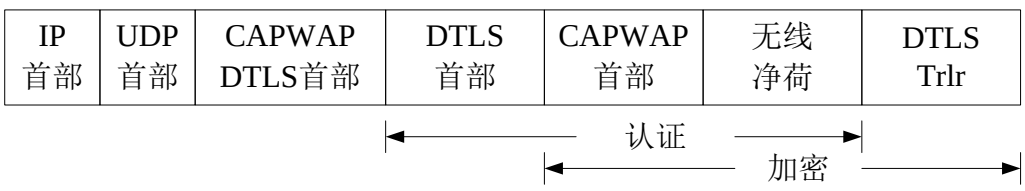
附图 2　CAPWAP Control Packet (DTLS Security Required)格式

作为选项，CAPWAP 协议允许使用 DTLS 保护数据分组。根据 AC 策略决定是否采用数据分组保护。当使用 DTLS 时，可选的 CAPWAP DTLS Header 存在，第 4-2 节介绍它。CAPWAP Data 分组格式如附图 3 所示。

CAPWAP Plain Text Data Packet :

IP 首部	UDP 首部	CAPWAP 首部	无线 净荷

DTLS Secured CAPWAP Data Packet :



附图 3　CAPWAP Data 分组格式

UDP Header：所有 CAPWAP 分组或者被封装在 UDP 内，或者如果使用 IPv6 被封装在 UDP-Lite 内。第 3 章定义特定 UDP 或 UDP-Lite 应用。

CAPWAP DTLS Header：加密 CAPWAP 协议分组的所有 DTLS 用 CAPWAP DTLS Header 添作前缀(参阅第 4-2 节)。

DTLS Header：DTLS Header 对被它封装的 CAPWAP 净荷提供认证和加密业务。DTLS 协议在[RFC4347]中定义。

CAPWAP Header：所有 CAPWAP 协议分组使用共同的首部，它紧跟 CAPWAP 前导或 DTLS 首部。CAPWAP Header 在第 4-3 节定义。

Wireless Payload：包含无线净荷的 CAPWAP 协议分组是 CAPWAP Data 分组。CAPWAP 协议没有规定无线净荷的格式，它由适当的无线标准定义。补充信息参阅第 4-4 节。

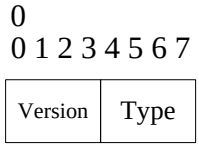
Control Header：CAPWAP 协议包括信令分量，称作 CAPWAP Control 协议。所有 CAPWAP Control 分组都包括 Control Header，它在第 4-5-1 节定义。CAPWAP Data 分组不包括 Control Header 字段。

Message Elements：CAPWAP Control 分组包括一个或多个消息要素，消息要素紧跟在 Control Header 后。这些消息要素位于 Type/Length/Value 类首部中，在第 4-6 节定义。

CAPWAP 实现**必须**能够接收长度为 4096 字节的重组的 CAPWAP 消息。通过在 Join Request 消息或 Join Response 消息中包括 Maximum Message Length 消息要素，CAPWAP 实现**可以**指出它支持更大的最大消息长度，参阅第 4-6-31 节。

4-1 CAPWAP 前导

CAPWAP 前导对于所有 CAPWAP 传输首部是通用的，并且用于标识跟在其后的首部类型。这个前导的作用是避免通过字节比较，来猜测是否这一帧是 DTLS 加密帧。它也提供可用于支持补充传输类型的扩展架构。前导格式如附图 4 所示。



附图 4 前导格式

Version：4 位字段，它包括这个分组使用的 CAPWAP 版本。这个规范的版本编号为 0。

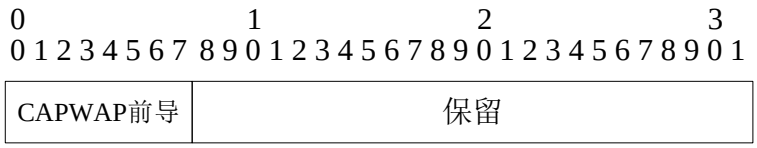
Type：4 位字段，它规定跟在 UDP 首部后面的净荷类型。支持下述值：

0 - CAPWAP Header。CAPWAP Header(参阅第 4-3 节)紧跟在 UDP 首部后。如果分组是在 CAPWAP Data 通道上收到的，CAPWAP 栈**必须**将该分组看作明文 CAPWAP Data 分组。如果分组是在 CAPWAP Control 通道上收到的，CAPWAP 栈**必须**将该分组看作明文 CAPWAP Control 分组。如果该控制分组既不是 Discovery Request 又不是 Discovery Response 分组，**必须**丢弃该分组。

1- CAPWAP DTLS Header。CAPWAP DTLS Header(和 DTLS 分组)紧跟在 UDP 首部后(参阅第 4-2 节)。

4-2 CAPWAP DTLS 首部

CAPWAP DTLS Header 用于识别被 DTLS 加密的分组。前 8 位包括公共 CAPWAP Preamble。其余 24 位用于填充确保 4 字节对齐，以及**可以**留作将来版本的协议使用。DTLS 分组[RFC4347]总是紧跟在这个首部之后。CAPWAP DTLS Header 格式如附图 5 所示。



附图 5　CAPWAP DTLS Header 格式

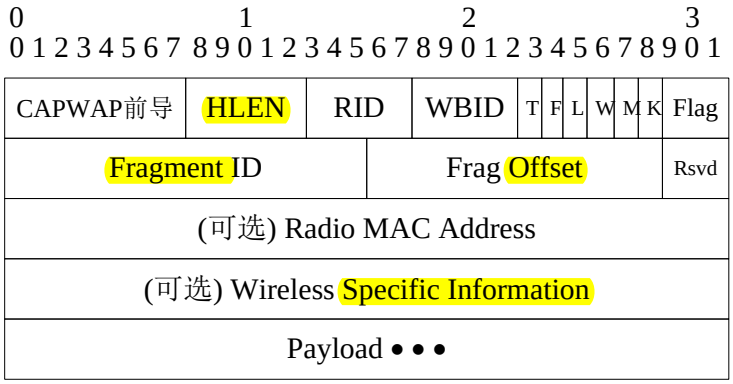
CAPWAP Preamble：CAPWAP Preamble 在第 4-1 节定义。CAPWAP Preamble 的 Payload Type 字段**必须**置 1。

Reserver：此 24 位字段保留将来使用。所有遵循这个协议的实现**必须**将由该实现支持的协议版本中保留的任何位设置为 0。接收方**必须**忽略不是为它们支持的协议版本定义的所有位。

4-3　CAPWAP 首部

所有 CAPWAP 协议消息用共同的首部格式封装，与使用 CAPWAP Control 或 CAPWAP Data 传输方式携带消息无关。然而，某些标志不适用于给定的传输。为了确定哪些标志合法，请参考介绍特定传输的节。

注意，本节中定义的可选字段**必须**有附图 6 所示精确次序。CAPWAP Header 格式如附图 6 所示。



附图 6　CAPWAP Header 格式

CAPWAP Preamble：CAPWAP Preamble 在第 4-1 节定义。CAPWAP Preamble 的 Payload Type 字段**必须**设置为 0。如果 CAPWAP DTLS Header 存在，在两个 CAPWAP Preambles 中的版本号**必须**匹配。采用这个重复字段的原因是避免对前导中版本字段的任何可能篡改，该前导没有被加密或认证。

HLEN：包括在 4 字节字中 CAPWAP 传输首部长度的 5 位字段(类似 IP 首部长度)。这个长度包括那些可选首部。

RID：5 位字段，包含这个分组的 Radio ID 号，在 1 和 31 之间取值。考虑到在 WTP 中多个物理无线电设备间的 MAC Addresses 不一定唯一，Radio Identifier (RID)字段用于指出此消息与哪个物理无线电设备关联。

WBID：5 位字段，是无线绑定标识符。此标识符指出与此无线电设备关联的无线分组的类型。为 WBID 定义有下述值：

0 – 保留

1- IEEE 802.11

2 – 保留

3 - EPCGlobal [EPCGlobal]

T：Type“T”位指出正在净荷中传送的帧的格式。此位为 1，净荷有由 WBID 字段指出的本地帧格式。为 0，净荷是 IEEE 802.3 帧。

F：Fragment“F”位指出是否这个分组是分段。此位为 1，分组为分段，并且**必须**与其他相应分段组合，以便重组成 WTP 和 AC 间交换的完整信息。

L：仅当“F”设置为 1 并且指出是否分组包括 WTP 和 AC 间分段交换的最后一个分段时，Last“L”位有效。此位为 1，分组是最后一个分段。此位为 0，分组不是最后一个分段。

W：Wireless“W”位用于规定在此首部中可选的 Wireless Specific Information 字段是否存在。此位值为 1 表示该可选字段(译注：此处原文单词为 header。按 field 翻译)存在。

M：Radio MAC“M”位用于指出存在 Radio MAC Address 可选首部。这用于传递接收无线电设备的 MAC 地址。

K：Keep-Alive“K”位指出分组是 Data Channel Keep-Alive 分组。这个分组用于映射数据通道到指定 Session ID 的控制通道，以及保持数据通道及时更新。对于包含用户数据的数据分组，“K”位**必须不能**置 1。

Flags：在 CAPWAP Header 中一组用于将来标志的保留位。遵循这个协议的所有实现**必须**将由该实现支持的协议版本中保留的任何位设置为 0。接收方**必须**忽略不是为它们支持的协议版本定义的所有位。

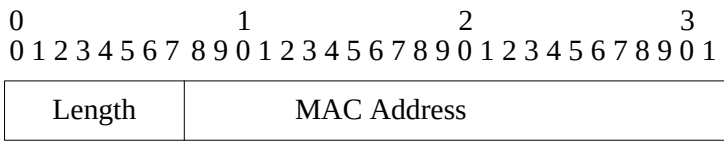
Fragment ID：16 位字段，它的值被分配给构成整个集合的每一组分段。Fragment ID 空间在每个 WTP/AC 对的每个方向上单独管理。Fragment ID 的值随每个新分段组增加。在其最大值已经用于标识一组分段后，Fragment ID 环回到 0。

Fragment Offset：13 位字段，指出在净荷中，重组期间这个分段的归属。如果“F”设置为 1，这个字段有效。分段偏移以 8 位位组(64 比特)为单位测量。第一个分段偏移为零。注意，CAPWAP 协议不允许重叠分段。

Reserved：3 位字段，保留将来使用。遵循这个协议的所有实现**必须**将由该实现支持的协议版本中保留的任何位设置为 0。接收方**必须**忽略不是为它们支持的协议版本定义的所有位。

Radio MAC Address：这个可选字段包括接收该分组的无线电设备的 MAC 地址。因为本地无线帧格式转换到 IEEE 802.3 格式会引起 WTP 的无线设备 MAC 地址丢失，这个字段使该地址能够传递给 AC。仅当“M”设置为 1，这个字段存在。HLEN 字段假设 4 字节对齐，如果不是这样，这个字段**必须**用 0(0x00)填充。

此字段基本格式如附图 7 所示。



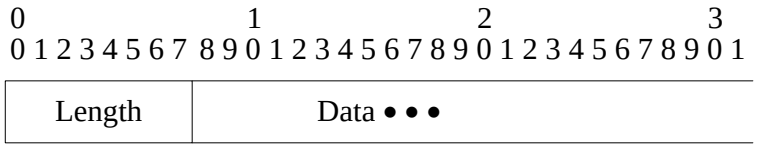
附图 7　Radio MAC Address 字段格式

Length：MAC 地址字段长度。支持在[EUI-48]和[EUI-64]中规定的格式和长度。

MAC 地址：接收无线电设备的 MAC 地址。

Wireless Specific Information：这个可选字段包括可用于携带 perpacket 无线信息的特定技术信息。仅当“W”位设置为 1 才有这个字段。在 CAPWAP Header 中的 WBID 字段用于标识 Wireless-Specific Information 可选字段的格式。HLEN 字段假设 4 字节对齐，如果不是这样，这个字段**必须**用 0(0x00)填充。

Wireless-Specific Information 字段格式如附图 8 所示。



附图 8　Wireless-Specific Information 字段格式

Length：此 8 位字段包括数据字段长度，最大值为 255。

Data:特定无线信息，由在 CAPWAP Header 的 WBID 字段中指定的特定无线绑定定义。

Payload：这个字段包括 CAPWAP Data Message 或 CAPWAP Control Message 首部，再加上消息中包含的数据。

4-4　CAPWAP 数据消息

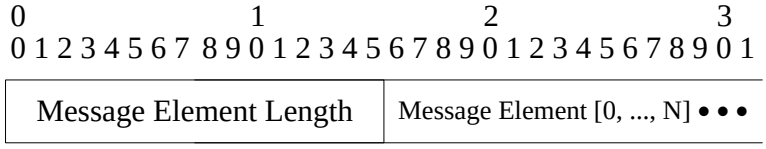
有两类不同的 CAPWAP Data 分组：CAPWAP Data Channel Keep-Alive 分组和 Data Payload 分组。前一类由 WTP 用于同步控制通道和数据通道，以及保持数据通道及时更新。第二类用于在 AC 和 WTP 间发送用户净荷。这一节介绍这两类 CAPWAP Data 分组格式。两类 CAPWAP Data 消息在 CAPWAP Data 通道上发送。

4-4-1　CAPWAP 数据通道保持激活

CAPWAP Data Channel Keep-Alive 分组用于利用数字通道绑定 CAPWAP 控制通道，并维持数据通道及时更新，确保该数据通道一直可用。当 DataChannelKeepAlive 计时器(参阅第 4-7-2 节)到期，WTP 发送 CAPWAP Data Channel Keep-Alive 分组。发送 CAPWAP Data Channel Keep-Alive 时，WTP 将 DataChannelDeadInterval 计时器置 1。一旦发送，在 CAPWAP Data Channel Keep-Alive 分组内 CAPWAP Header 中的所有字段，除了 HLEN 字段和“K”位以外，都设置为 0。一旦收到 CAPWAP Data Channel Keep-Alive 分组，AC 返回 CAPWAP Data Channel Keep-Alive 分组给 WTP。AC 返回分组内容与收到分组内容相同。

一旦收到CAPWAP Data Channel Keep-Alive分组，WTP解除DataChannelDeadInterval计时器并复位DataChannelKeepAlive计时器。WTP重传CAPWAP Data Channel Keep-Alive分组，采用的方法和发送CAPWAP Control消息相同。如果DataChannelDeadInterval计时器到期，WTP拆除控制DTLS会话，如果存在数据DTLS会话，也将拆除。

CAPWAP Data Channel Keep-Alive 分组包括后面紧随 CAPWAP Header 的净荷(参阅第 4-3 节)。CAPWAP Data Channel Keep-Alive 分组格式如附图 9 所示。



附图 9　CAPWAP Data Channel Keep-Alive 分组格式

Message Element Length：16 位 Length 字段，指出在 CAPWAP Header 后的字节数，最大 65535 字节。

Message Element[0..N]：消息要素携带与每个 CAPWAP Data Channel Keep-Alive 消息有关的信息。下述消息要素**必须**出现在这个 CAPWAP 消息中：

Session ID，参阅第 4-6-37 节。

4-4-2　数据净荷

CAPWAP protocol Data Payload 分组封装转发的无线帧。CAPWAP 协议定义两种不同的封装模式：IEEE 802.3 和本地无线。IEEE 802.3 封装要求，对于 802.11 帧，在 WTP 中执行 802.11 *Integration*功能。采用 IEEE 802.3 封装的用户净荷有附图 10 所示的格式。

IP Header	UDP Header	CAPWAP Header	802.3 Frame

附图 10　采用 IEEE 802.3 封装的用户净荷格式

CAPWAP协议也定义本地无线封装模式。封装的CAPWAP Data帧格式服从由绑定的特定无线技术规定的规则。每个绑定的无线技术**必须**有标题为“Payload Encapsulation”的一节，该节定义在CAPWAP Data分组中封装的无线净荷格式。

对于802.3净荷帧，封装的是802.3帧(不包括IEEE 802.3 Preamble、Start Frame Delimiter (SFD)和Frame Check Sequence (FCS)字段)。如果被封装帧超过传输层的MTU，发送方负责分段该帧，如第3-4节规定的。CAPWAP协议可以支持这样的IEEE 802.3帧，它们的长度在作为规范[FRAME-EXT]的IEEE 802.3中定义。

4-4-3　建立 DTLS 数据通道

如果配置 AC 和 WTP 在 DTLS 上隧道化数据通道，必须发起适当的 DTLS 会话。为了避免必须认证和授权 AC 和 WTP，**应当**使用 TLS 会话重新开始功能[RFC5246]启动 DTLS 数据通道。对于没有激活的控制通道会话的 DTLS 会话，AC DTLS 实现**必须不能**发起数据通道会话。

4-5　CAPWAP 控制消息

CAPWAP Control 协议在 WTP 和 AC 间提供控制通道。控制消息有下述消息类型：

Discovery：CAPWAP Discovery 消息用于识别潜在的 AC，它们的负载和能力。

Join：WTP 使用 CAPWAP Join 消息请求 AC 服务，AC 响应 WTP。

Control Channel Management：CAPWAP Control 通道管理消息用于维持控制通道。

WTP Configuration Management：WTP Configuration 消息由 AC 用于传递指定的配置给 WTP。从 WTP 获取统计资料的消息也包括在 WTP Configuration Management 中。

Station Session Management：Station Session Management 消息由 AC 用于传递规定的站策略给 WTP。

Device Management Operations：设备管理操作用于请求和传递固件映像给 WTP。

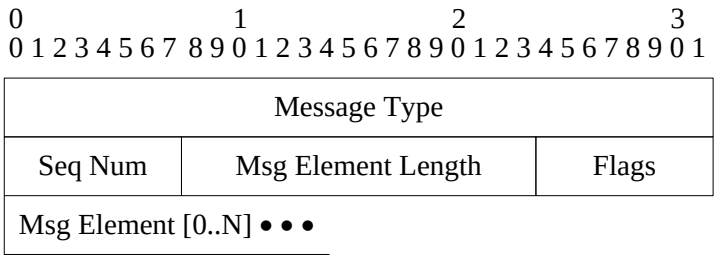
Binding-Specific CAPWAP Management Messages：这一类别消息由 AC 和 WTP 使用，用于交换特定协议的 CAPWAP 管理消息。这些消息可能改变，或可能不改变站的链路状态。

必须实现 Discovery、Join、Control Channel Management、WTP Configuration Management 和 Station Session Management CAPWAP Control 消息。**可以**实现 Device Management Operations 消息。

从 WTP 发送到 AC 的 CAPWAP Control 消息指出 WTP 可以使用，为 WTP 提供隐含的保持激活机制。当没有交换其他 CAPWAP Control 消息时，Control Channel Management Echo Request 和 Control Channel Management Echo Response 消息提供显式保持激活机制。

4-5-1　控制消息格式

所有 CAPWAP Control 消息被封装在 CAPWAP Header 中发送(参阅第 4-3 节)。紧跟在 CAPWAP Header 之后的是控制首部，控制首部格式如附图 11 所示。



附图 11　控制首部格式

4-5-1-1　消息类型

Message Type 字段指出 CAPWAP Control 消息的功能。为了有可扩展性，Message Type 字段由 IANA Enterprise Number [RFC3232]和企业特定消息类型编码构成。前 3 个八位位组包含 IANA Enterprise Number，采用网络字节顺序，0 用于定义消息类型的 CAPWAP 基本协议(这个规范)。最后的八位位组是企业特定消息类型编码，它的取值范围从 0 到 255。

Message Type 字段定义为：

Message Type =

IANA Enterprise Number × 256 +

Enterprise Specific Message Type Number

CAPWAP 协议可靠性机制要求成对定义消息，由 Request 和 Response 消息构成。Response 消息**必须**确认 Request 消息。总是成对分配 CAPWAP Control Message Type Values。所有 Request 消息有奇数编码的 Message Type Values，所有 Response 消息有偶数编码的 Message Type Values。**必须**先分配 Request 值。例如，为 Request 消息分配值为 3 的 Message Type Value，为 Response 消息分配值为 4 的 Message Type Value 是合法的；而为 Response 消息分配值为 4 的 Message Type Value，为 Request 消息分配值为 5 的 Message Type Value 是不合法的。

当 WTP 或 AC 收到消息，该消息的 Message Type Value 字段不能识别并且是奇数，在 Message Type Value Field 中的数加 1，带有包含该增加值的 Message Type Value 字段和包含带有该值(Unrecognized Request)的 Result Code 消息要素的 Response 消息被返回给所接收消息的发送方。如果未知的消息类型是偶数，忽略该消息。

CAPWAP Control Message Types的合法取值在下表中规定：

CAPWAP Control Message	Message Type Value
Discovery Request	1
Discovery Response	2
Join Request	3
Join Response	4
Configuration Status Request	5
Configuration Status Response	6
Configuration Update Request	7
Configuration Update Response	8
WTP Event Request	9
WTP Event Response	10
Change State Event Request	11
Change State Event Response	12
Echo Request	13

Echo Response	14
Image Data Request	15
Image Data Response	16
Reset Request	17
Reset Response	18
Primary Discovery Request	19
Primary Discovery Response	20
Data Transfer Request	21
Data Transfer Response	22
Clear Configuration Request	23
Clear Configuration Response	24
Station Configuration Request	25
Station Configuration Response	26

4-5-1-2 序列号

Sequence Number 字段是标识符值，用于匹配 Request 和 Response 分组。当收到带有 Request Message Type Value 的 CAPWAP 分组时，Sequence Number 字段的值被复制到相应的 Response 消息中。

当发送 CAPWAP Control 消息时，发送方的内部序列号计数器单调增加，确保不会出现两个未定的 Request 消息有相同序列号。Sequence Number 字段环回到 0。

4-5-1-3 消息要素长度

此 Length 字段指出 Sequence Number 字段后的字节数。

4-5-1-4 标志

必须将 Flags 字段设置为 0。

4-5-1-5 消息要素[0..N]

消息要素携带与每个控制消息类型有关的信息。在本规范中的每个控制消息规定哪些消息要素是合法的。

当 WTP 或 AC 收到 CAPWAP 消息，而该消息不携带按规定它必须携带的消息要素，那么，抛弃此 CAPWAP 消息。如果收到的消息是 Request 消息，与该消息相对应的 Response 消息携带消息要素，那么，将对应的 Response 消息(该消息带有指出“Failure - Missing Mandatory Message Element”的 Result Code 消息要素)返回给发送方。

当 WTP 或 AC 收到 CAPWAP 消息，该消息带有 WTP 或 AC 不能识别的消息要素，抛弃该 CAPWAP 消息。如果收到的消息是 Request 消息，与该消息对应的 Response 消息携带消息要素，那么，对应的 Response 消息(该消息带有指出“Failure - Unrecognized Message Element”的 Result Code 消息要素和一个或多个 Returned Message Element 消息要素)包括在内，包含不能识别的消息要素。

4-5-2 服务质量

CAPWAP 基本协议不提供任何用于 CAPWAP Data 消息的服务质量(Quality of Service, QoS)建议。任何有 QoS 要求的特定无线 CAPWAP 绑定规范**必须**定义应用于 CAPWAP Data 消息的 QoS 要求。

IP 首部也包括 Explicit Congestion Notification (ECN)位[RFC3168]。[RFC3168]的第 9-1-1 节介绍了两个层次的 ECN 功能：全部功能和有限功能。CAPWAP ACs 和 WTPs **将**实现有限功能，**建议**实现在[RFC3168]中介绍的全部功能。

4-5-2-1 在 CAPWAP 控制消息中应用 QoS

建议由 AC 和 WTP 发送的 CAPWAP Control 消息采用适当的 QoS 优先权值，确保 CAPWAP Control 通道尽可能不会因网络拥塞断开。因此，开启 QoS 的 CAPWAP 设备**应当**使用下述值：

802.1Q：**应当**使用优先权标记 7。

DSCP：**应当**使用 CS6 每跳 Service Class，它在[RFC2474]中介绍。

4-5-3 重传

CAPWAP Control 协议是一款可靠传输协议。对于每个 Request 消息，都相应规定有 Response 消息，用于确认收到 Request 消息。此外，控制首部 Sequence Number 字段用于配对 Request 消息和 Response 消息(参阅第 4-5-1 节)。

不精确确认 Response 消息；因此，如果没有收到 Response 消息，重传原始 Request 消息。

实现**必须**跟踪最后收到的 Request 消息的序列号，**必须**缓存相应的 Response 消息。如果收到具有相同序列号的重传，**必须**重传缓存的 Response 消息，并且不重新处理该 Request。如果收到较旧的 Request 消息，说明该消息的序列号较小，**必须**忽略该消息。收到较新的 Request 消息，说明该消息序列号较大，按正常情况处理该消息。

注意：当且仅当(s1<s2 和(s2-s1)<128)或(s1>s2 和(s1-s2)>128)时，如果 s1 小于 s2 模 256，认为序列号“较小”。

在任何给定时间，WTP 和 AC 都仅有单个未解决的请求。发送方**必须不能**改变 Retransmitted Request 消息。

发送 Request 消息后，由 RetransmitInterval(参阅第 4-7 节)计时器和 MaxRetransmit(参阅第 4-8 节)变量决定是否需要重传原始 Request 消息。RetransmitInterval 计时器用于首次 Request 重传。以后每一次重传相同 Request 消息该计时器重传间隔时间加倍，直到 MaxRetransmit，但是不超过 EchoInterval 计时器(参阅第 4-7-7 节)时间一半。Response 消息不受这些计时器约束。

如果发送方在达到 MaxRetransmit 次重传前停止重传 Request 消息(这会导致转换到 DTLS Teardown，如第 2-3-1 节所述)，发送方不知道接收方是收到和处理了该 Request 还是没有。在大多数情况，发送方**不应当**这样做，而应当继续重传直到收到 Response 消息，或到 DTLS Teardown 转换发生。然而，如果发送方决定继续与新的或修改过的 Request 消息连接，新消息**必须**有新序列号，并被看作是来自接收方的新 Request 消息。注意，WTP 和 AC 的序列号很可能变得不同步。

当重传 Request 消息时，该消息**必须**经 DTLS 栈重新加密。如果对端已经收到 Request 消息，并且相应的 Response 消息丢失，必须确保重传的 Request 消息不被视为 DTLS 栈的重放。类似，任何缓存的 Response 消息(由于收到重传的 Request 消息而被重传)必须经 DTLS 重新加密。

Duplicate Response 消息，由在 CAPWAP Control 消息首部中 Sequence Number 字段标识，一旦收到**应当**抛弃。

4-6 CAPWAP 协议消息要素

这一节定义包含在 CAPWAP 协议控制消息中的 CAPWAP Protocol 消息要素。

消息要素用于携带控制消息中需要的信息。每个消息要素由 Type Value 字段标识，如下面定义。在消息要素的长度字段指出消息要素的总长度。

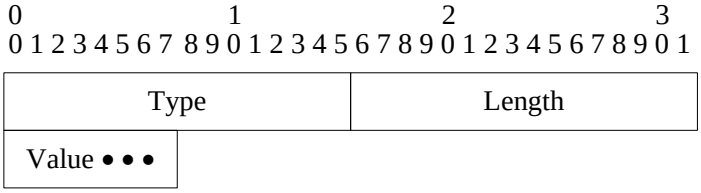
本文档中所有消息要素定义使用类似于下面的格式图来描述消息要素的格式。注意，为了简化本文档的介绍，这些格式图不包括首部字段(Type 和 Length)。在消息要素介绍中定义首部字段值。

除非另有规定，控制消息(它列出一组支持的(或期盼的)消息要素)，**必须不**指望这些消息要素以任何规定的次序出现。发送方**可以**以任何次序包括消息要素。除非另有说明，在给定的控制消息中每类消息要素只有一个。

除非另有规定，由 AC 发送给 WTP 的任何配置信息**可以**保存到非易失性存储器中(更多信息参阅第 8-1 节)。

在独立的 IETF 文档中可以定义补充消息要素。

消息要素格式使用如附图 12 所示的 TLV 格式。



附图 12 TLV 格式

16 位 Type 字段标识 Value 字段携带的信息，Length(16 位)指出 Value 字段的字节数。0 值保留并且**不能**使用。字段值其余部分分配如下：

用途	类型值
CAPWAP Protocol Message Elements	1 - 1023
IEEE 802.11Message Elements	1024 – 2047
保留将来使用	2048 – 3071
EPCGlobalMessage Elements	3072 – 4095
保留将来使用	4096 – 65535

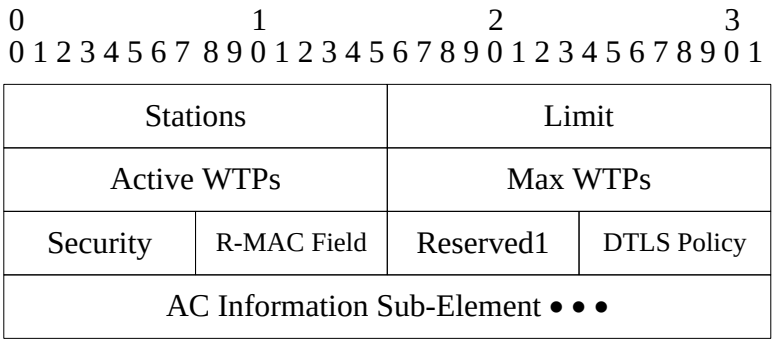
下表列出 CAPWAP 协议消息要素(Message Elements)和它们的 Type 值。

CAPWAP消息要素(Message Element)	类型值(Type Value)
AC Descriptor	1
AC IPv4 List	2
AC IPv6 List	3
AC Name	4
AC Name with Priority	5
AC Timestamp	6
Add MAC ACL Entry	7
Add Station	8
Reserved	9
CAPWAP Control IPV4 Address	10
CAPWAP Control IPV6 Address	11
CAPWAP Local IPV4 Address	30
CAPWAP Local IPV6 Address	50

CAPWAP Timers 12
CAPWAP Transport Protocol 51
Data Transfer Data 13
Data Transfer Mode 14
Decryption Error Report 15
Decryption Error Report Period 16
Delete MAC ACL Entry 17
Delete Station 18
Reserved 19
Discovery Type 20
Duplicate IPv4 Address 21
Duplicate IPv6 Address 22
ECN Support 53
Idle Timeout 23
Image Data 24
Image Identifier 25
Image Information 26
Initiate Download 27
Location Data 28
Maximum Message Length 29
MTU Discovery Padding 52
Radio Administrative State 31
Radio Operational State 32
Result Code 33
Returned Message Element 34
Session ID 35
Statistics Timer 36
Vendor Specific Payload 37
WTP Board Data 38
WTP Descriptor 39
WTP Fallback 40
WTP Frame Tunnel Mode 41
Reserved 42
Reserved 43
WTP MAC Type 44
WTP Name 45
Unused/Reserved 46
WTP Radio Statistics 47
WTP Reboot Statistics 48
WTP Static IP Address Information 49

4-6-1 AC 描述符

AC Descriptor 消息要素由 AC 用于通知它目前的状态。该值包括如附图 13 所述的字段。



附图 13　AC 描述符格式

Type：　AC Descriptor 为 1

Length：>= 12

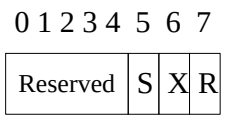
Stations：目前 AC 服务的站数目

Limit：AC 最多可支持的站数目

Active WTPs：目前附着到 AC 的 WTPs 数目

Max WTPs：AC 最多可支持的 WTPs 数目

Security：8 位标记，规定 AC 支持的认证证书类型(参阅第 2-4-4 节)。该字段格式如附图 14 所示。



附图 14　Security 字段格式

Reserved：多个保留位留作将来使用。所有遵循这个协议的实现，对于该实现支持的协议版本中的任何保留位，**必须**设置为 0。接收方**必须**忽略所有不是为接收方支持协议版本定义的位。

S：AC 支持预共享秘密认证，如第 12-6 节所述。

X：AC 支持 X.509 Certificate 认证，如第 12-7 节所述。

R：保留位，留作将来使用。所有遵循这个协议的实现，对于该实现支持的协议版本中的任何保留位，**必须**设置为 0。接收方**必须**忽略所有不是为接收方支持协议版本定义的位。

R-MAC Field：AC 支持 CAPWAP 传输首部(参阅第 4-3 节)中可选的 Radio MAC Address 字段。支持下述枚举值：

0 – 保留

1 – 支持

2 – 不支持

Reserved：一组留作将来使用的保留位。所有遵循这个协议的实现，对于该实现支持的协议版本中的任何保留位，**必须**设置为 0。接收方**必须**忽略所有不是为接收方支持协议版本定义的位。

DTLS Policy：AC 用此通知它对于 CAPWAP 数据通道 DTLS 应用的策略。AC **可以**通知不止一个支持选项，由下面的位字段表示。WTP **必须**服从 AC 通知的选项中的一个。该字段格式如附图 15 所示。

0 1 2 3 4 5 6 7

Reserved	D	C	R

附图 15　DTLS Policy 字段格式

Reserved：一组留作将来使用的保留位。所有遵循这个协议的实现，对于该实现支持的协议版本中的任何保留位，**必须**设置为 0。接收方**必须**忽略所有不是为接收方支持协议版本定义的位。

D：DTLS-Enabled Data Channel Supported

C：Clear Text Data Channel Supported

R：留作将来使用的保留位。所有遵循这个协议的实现，对于该实现支持的协议版本中的任何保留位，**必须**设置为 0。接收方**必须**忽略所有不是为接收方支持协议版本定义的位。

AC Information Sub-Element：AC Descriptor 消息要素包含多个 AC Information 子要素，定义了两种子类型，它们**必须**一个都不能少。AC Information 子要素格式如附图 16 所示。

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

AC Information Vendor Identifier	
AC Information Type	AC Information Length
AC Information Data ● ● ●	

附图 16　AC Information 子要素格式

AC Information Vendor Identifier：32 位值，包括 IANA 分配的“Structure of Management Information (SMI) Network Management Private Enterprise Codes”。

AC Information Type：采用 UTF-8 格式[RFC3629]的供应商专有 AC 信息编码。支持下述枚举值。在 AC Descriptor 消息要素中**必须**包括 Hardware 版本子要素和 Software 版本子要素。下面列出的这些值连带着 AC Information Vendor Identifier 字段一起使用，这个字段的值**必须**设置为 0。这个字段，结合设置为非 0 值的 AC Information Vendor Identifier，允许供应商使用私有命名空间。

4 - Hardware Version：AC 硬件版本号。

5 - Software Version：AC 软件(固件)版本号。

AC Information Length：供应商专有 AC 信息编码长度，最大 1024。

AC Information Data：供应商专有 AC 信息编码。

4-6-2　AC IPv4 列表

AC IPv4 List 消息要素用于为 WTP 配置可供 WTP 加入的最新 ACs 列表。此消息要素格式如附图 17 所示。

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

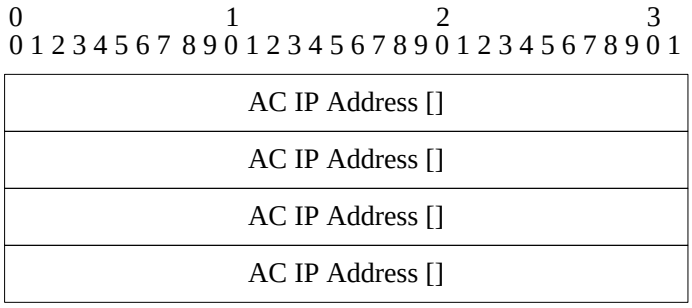
AC IP Address []

附图 17　AC IPv4 List 消息要素格式

Type：AC IPv4 List 为 2
Length：>= 4
AC IP Address：32 位整数阵列，包括 AC IPv4 Addresses，包括的地址不超过 1024 个。

4-6-3　AC IPv6 列表

AC IPv6 List 消息要素用于为 WTP 配置可供 WTP 加入的最新 ACs 列表。此消息要素格式如附图 18 所示。

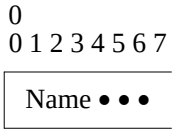


附图 18　AC IPv6 List 消息要素格式

Type：AC IPV6 List 为 3
Length：>= 16
AC IP Address：128 位整数阵列，包括 AC IPv6 Addresses，包括的地址不超过 1024 个。

4-6-4　AC 名称

AC Name 消息要素包含以 UTF-8 格式[RFC3629]表示的 AC 身份。此值是可变长度字节串。该串不以 0 终结。AC Name 消息要素格式如附图 19 所示。

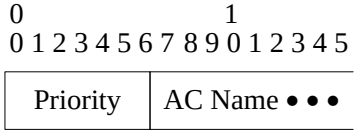


附图 19　AC Name 消息要素格式

Type：AC Name 为 4
Length：>= 1
Name：可变长度 UTF-8 编码串[RFC3629]，包含 AC 的名称，其最大长度**必须不能**超过 512 字节。

4-6-5　带优先权的 AC 名称

带 Priority 消息要素的 AC Name 由 AC 发送给 WTP，以便配置优先的 ACs。这个消息要素的实例数目等于在 WTP 上配置的 ACs 数目。WTP 也使用这个消息要素发送它自己的配置给 AC。带 Priority 消息要素的 AC Name 的格式如附图 19 所示。

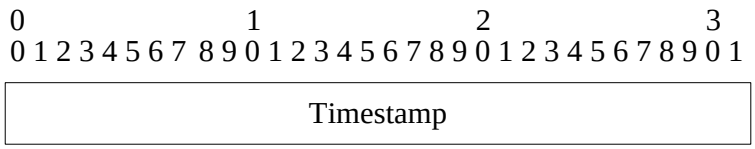


附图 19　带 Priority 消息要素的 AC Name 的格式

Type：AC Name with Priority 为 5
Length：>= 2
Priority：1 至 255 之间的值，规定首选 AC 的优先权顺序。例如，值 1 用于设置主要 AC，值 2 用于设置辅助 AC ，等等。
AC Name：可变长度 UTF-8 编码串[RFC3629]，包含 AC 的名称，其最大长度**必须不能**超过 512 字节。

4-6-6　AC 时间戳

AC Timestamp 消息要素由 AC 发送，用于同步 WTP 时钟。AC 时间戳要素的格式如附图 20 所示。

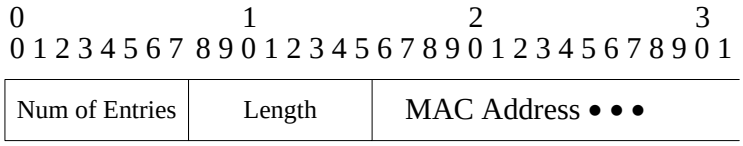


附图 20　AC Timestamp 消息要素格式

Type：AC Timestamp 为 6
Length：4
Timestamp：AC 的目前时间，让所有 WTPs，采用 Network Time Protocol (NTP) [RFC1305]中定义的格式，实现时间同步。仅 NTP 时间的最高有效 32 位包括在这个字段中。

4-6-7　添加 MAC ACL 条目

Add MAC Access Control List (ACL) Entry 消息要素由 AC 用于在 WTP 上添加 MAC ACL 列表条目，确保 WTP 不再为该消息中给出的 MAC 地址提供服务。不能预期这个消息要素中给出的 MAC 地址会保存在 WTP 的非易失性存储器中。每次 WTP 与 AC 建立新会话时，清除 WTP 上的 MCA ACL 表。Add MAC Access Control List (ACL) Entry 消息要素格式如附图 21 所示。



附图 21　Add MAC Access Control List (ACL) Entry 消息要素格式

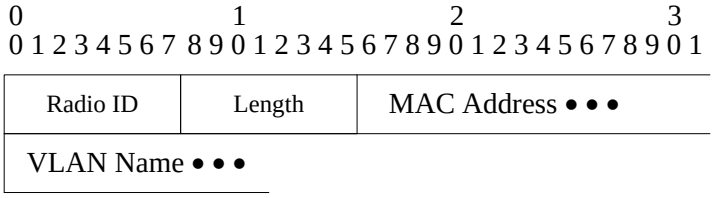
Type：Add MAC ACL Entry 为 7
Length：>= 8
Num of Entries：阵列中 Length/MAC Address 字段实例数目。此值**必须不能**超过 255。
Length：MAC Address 字段长度。支持采用[EUI-48]和[EUI-64]中规定的格式和长度。
MAC Address：添加到 ACL 的 MAC 地址。

4-6-8　添加站

Add Station 消息要素由 AC 用于通知 WTP 它应当转发站的流量。Add Station 消息要素伴随有特定技术绑定信息元素，这些元素可以包括安全参数。因此，该站的 WTP **必须**为该

站使用安全参数。

在通过 Add Station 消息要素将站策略传递给 WTP 后，通过发送修改的 Add Station 消息要素，AC **可以**改变任何策略。如果 WTP 收到针对已有站的 Add Station 消息要素，WTP **必须**重写该站的任何已有状态。Add Station 消息要素格式如附图 22 所示。



附图 22　Add Station 消息要素格式

Type：Add Station 为 8

Length：>= 8

Radio ID：8 位值，代表无线电设备，其值在 1 和 31 之间。

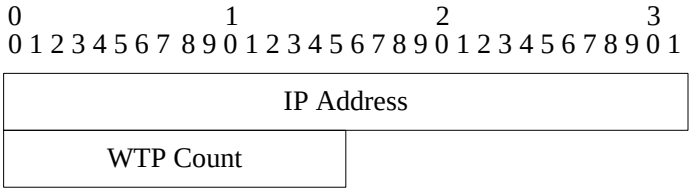
Length：MAC Address 字段长度。支持采用[EUI-48]和[EUI-64] 中规定的格式和长度。

MAC Address：站的 MAC 地址。

VLAN Name：可选的可变长度 UTF-8 编码串[RFC3629]，最大长度 512 个八位位组，包含 VLAN Name，在该 VLAN 上，WTP 将在本地桥接用户数据。注意，仅当采用 Local MAC 模式配置的 WTPs 时这个字段合法。

4-6-9　CAPWAP 控制 IPv4 地址

CAPWAP Control IPv4 Address 消息要素由 AC 在 Discovery 处理期间发送给 WTP，以及由 AC 用于提供该 AC 上的可用接口，和提供目前连接的 WTPs 数量。当返回多个 CAPWAP Control IPV4 Address 要素时，WTP **应当**跨多个接口进行负载均衡(参阅第 6-1 节)。CAPWAP Control IPv4 Address 消息要素格式如附图 23 所示。



附图 23　CAPWAP Control IPv4 Address 消息要素格式

Type：CAPWAP Control IPv4 Address 为 10

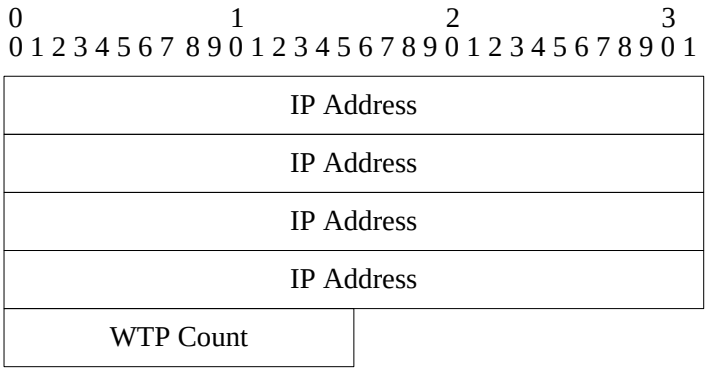
Length：6

IP Address：接口的 IP 地址。

WTP Count：目前连接到该接口的 WTPs 数目，最多 65535。

4-6-10　CAPWAP 控制 IPv6 地址

CAPWAP Control IPv6 Address 消息要素由 AC 在 Discovery 处理期间发送给 WTP，以及由 AC 用于提供该 AC 上的可用接口，和提供目前连接的 WTPs 数量。这个消息要素可供 WTP 跨多个接口进行负载均衡(参阅第 6-1 节)。CAPWAP Control IPv6 Address 消息要素格式如附图 24 所示。

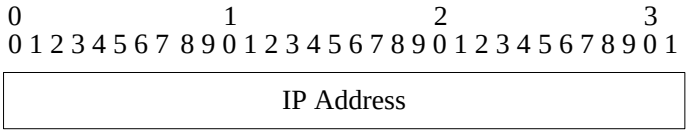


附图 24　CAPWAP Control IPv6 Address 消息要素格式

Type：CAPWAP Control IPv6 Address 为 11
Length：18
IP Address：接口的 IP 地址。
WTP Count：目前连接到该接口的 WTPs 数目，最多 65535。

4-6-11　CAPWAP 本地 IPv4 地址

CAPWAP Local IPv4 Address 消息要素或者由 WTP 在 Join Request 中发送，或者由 AC 在 Join Response 中发送。该消息要素用于传递发送方的 IP Address。接收方将该消息要素的值与分组的源 IP 地址比较，确定在两个对端间是否存在中间体(middlebox)。CAPWAP Local IPv4 Address 消息要素格式如附图 25 所示。

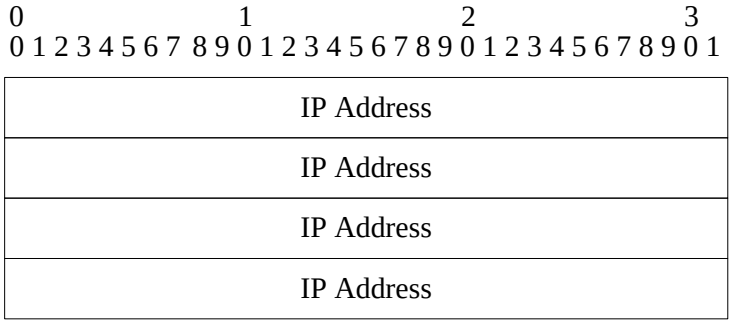


附图 25　CAPWAP Local IPv4 Address 消息要素格式

Type：CAPWAP Local IPv4 Address 为 30
Length：4
IP Address：发送方的 IP 地址。

4-6-12　CAPWAP 本地 IPv6 地址

CAPWAP Local IPv6 Address 消息要素或者由 WTP 在 Join Request 中发送，或者由 AC 在 Join Response 中发送。该消息要素用于传递发送方的 IP Address。接收方将该消息要素的值与分组的源 IP 地址比较，确定在两个对端间是否存在中间体。CAPWAP Local IPv6 Address 消息要素格式如附图 26 所示。

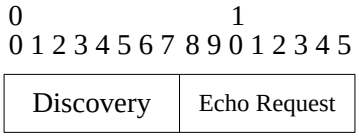


附图 26　CAPWAP Local IPv6 Address 消息要素格式

Type：CAPWAP Local IPv6 Address 为 50
Length：16
IP Address：发送方的 IP 地址。

4-6-13　CAPWAP 计时器

CAPWAP Timers 消息要素由 AC 用于配置 WTP 上的 CAPWAP 计时器。CAPWAP Timers 消息要素格式如附图 27 所示。



附图 27　CAPWAP Timers 消息要素格式

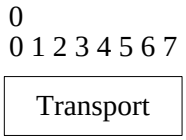
Type：CAPWAP Timers 为 12
Length：2
Discovery：当 WTP 处于 Discovery 阶段时，CAPWAP Discovery 消息间的秒数。用这个值配置 MaxDiscoveryInterval 计时器(参阅第 4-7-10 节)。
Echo Request：WTP Echo Request CAPWAP 消息间的秒数。用这个值配置 EchoInterval 计时器(参阅第 4-7-7 节)。AC 设置它的 EchoInterval 计时器到这个值，加上在第 4-5-3 节中介绍的最大重传时间。

4-6-14　CAPWAP 传输协议

如果 CAPWAP 在 IPv6 上运行，**可以**使用 UDP-Lite 或 UDP 传输(参阅第 3 章)。CAPWAP IPv6 Transport Protocol 消息要素由 WTP 或 AC 用于通报 CAPWAP 数据通道使用哪个传输协议。

一旦收到 Join Request，如果是在 IPv6 上收到此 CAPWAP 消息，并且 CAPWAP Local IPv6 Address 消息要素存在(参阅第 4-6-12 节)并且没有检测到中间体(参阅第 11 章)，AC **可以**在 Join Response 消息中，将 CAPWAP Transport Protocol 设置为 UDP-Lite。

任何其他情况，**必须**设置 CAPWAP Transport Protocol 为 UDP。CAPWAP Transport Protocol 消息要素格式如附图 28 所示。



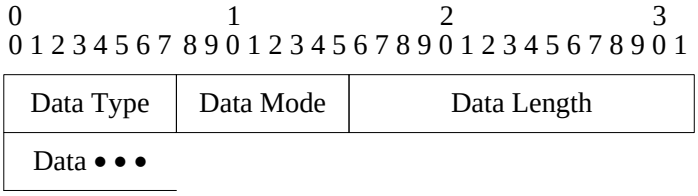
附图 28　CAPWAP Transport Protocol 消息要素格式

Type：CAPWAP Transport Protocol 为 51
Length：1
Transport：用于 CAPWAP Data 通道传输。支持下述枚举值：

1 - UDP-Lite：UDP-Lite 传输协议用于 CAPWAP Data 通道。注意，如果是在 IPv4 上使用 CAPWAP Control 通道，**不能**使用这个选项。
2 - UDP：UDP 传输协议用于 CAPWAP Data 通道。

4-6-15 数据传输数据

Data Transfer Data 消息要素由 WTP 用于提供信息给 AC，用于调试。Data Transfer Data 消息要素格式如附图 29 所示。



附图 29 Data Transfer Data 消息要素格式

Type：Data Transfer Data 为 13

Length：>= 5

Data Type：8 位值，表示传输 Data Type。支持下述枚举值：

1 – 包括传输数据。

2 – 包括最后一个 Transfer Data Block(文件结束(End of File (EOF))。

5 – 错误发生。传输被终止。

Data Mode：8 位值，描述正在传输的信息类型。支持下述枚举值：

0 – 保留

1 – WTP Crash Data

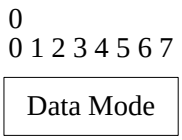
2 - WTP Memory Dump

Data Length：数据字段长度，最大值为 65535。

Data：正在从 WTP 传送到 AC 的数据，数据类型由 Data Mode 字段标识。

4-6-16 数据传输模式

Data Transfer Mode 消息要素由 WTP 用于指出它正在发送到 AC，用于调试的数据传输信息类型。Data Transfer Mode 消息要素格式如附图 30 所示。



附图 30 Data Transfer Mode 消息要素格式

Type：Data Transfer Mode 为 14

Data Mode：8 位值，描述要求的信息类型。支持下述枚举值：

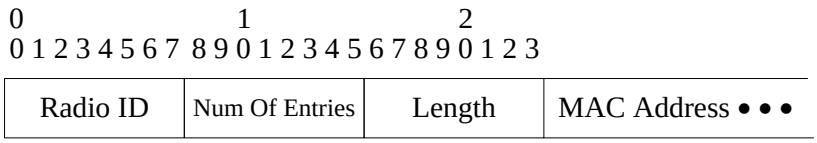
0 – 保留：

1 - WTP Crash Data

2 - WTP Memory Dump

4-6-17 解密错误报告

Decryption Error Report 消息要素的值由 WTP 用于通知解密出错的 AC，这些错误是自上次报告以来发生的。注意，如果是在 AC 中提供加密和解密业务，不使用这个错误报告机制。Decryption Error Report 消息要素格式如附图 31 所示。

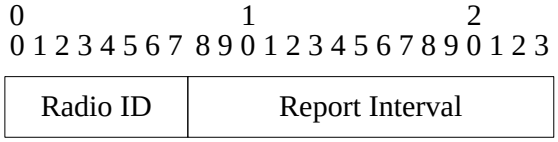


附图 31　Decryption Error Report 消息要素格式

Type：Decryption Error Report 为 15
Length：>= 9
Radio ID：Radio Identifier 指 WTP 上的接口索引，其值在 1 和 31 间。
Num of Entries：阵列中 Length/MAC Address 字段的实例数。这个字段**必须不能**超过 255。
Length：MAC Address 字段长度。支持采用[EUI-48]和[EUI-64]中规定的格式和长度。
MAC Address：引发解密错误的站的 MAC address。

4-6-18　解密错误报告周期

Decryption Error Report Period 消息要素值由 AC 用于通知 WTP，它应当多长时间发送一次解密错误报告消息。注意，如果是在 AC 中提供加密和解密业务，不使用这个错误报告机制。Decryption Error Report Period 消息要素格式如附图 32 所示。

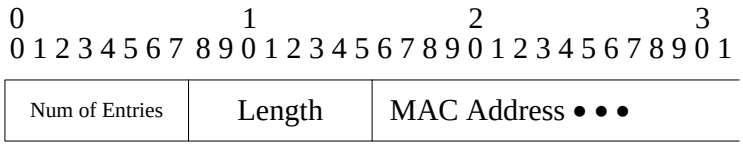


附图 32　Decryption Error Report Period 消息要素格式

Type：Decryption Error Report Period 为 16
Length：3
Radio ID：Radio Identifier 指 WTP 上的接口索引，其值在 1 和 31 间。
Report Interval：16 位无符号整数，指出时间，单位为秒。这个消息要素的默认值可在第 4-7-11 节找到。

4-6-19　删除 MAC ACL 条目

Delete MAC ACL Entry 消息要素由 AC 用于在 WTP 上删除 MAC ACL 条目，确保 WTP 向在该消息中给出的 MAC 地址提供服务。Delete MAC ACL Entry 消息要素格式如附图 33 所示。



附图 33　Delete MAC ACL Entry 消息要素格式

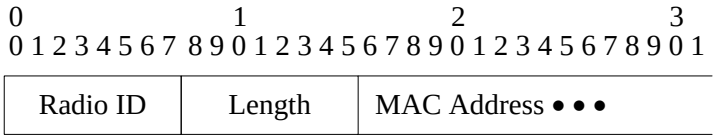
Type：Delete MAC ACL Entry 为 17
Length：>= 8
Num of Entries：在阵列中 Length/MAC Address 字段的实例数。这个字段**必须不能**超过 255。
Length：MAC Address 字段长度。支持[EUI-48]和[EUI-64]中规定的格式和长度。
MAC Address：从 ACL 中删除的 MAC 地址阵列。

4-6-20 删除站

Delete Station 消息要素由 AC 用于通知 WTP，它不应当再对特定站提供服务。一旦收到这个消息要素 WTP **必须**立即终止对该站的服务。

有多种原因会导致发送 Delete Station 消息要素，包括管理原因，或者如果站已经漫游到另一个 WTP。

Delete Station 消息要素**可以**由 WTP 在 WTP Event Request 消息中发送，以便通知 AC，不再向特定站提供服务。这将作为 Idle Timeout 的结果发生(参阅第 4-4-43 节)，可能是内部资源短缺或其他原因。Delete Station 消息要素格式如附图 34 所示。

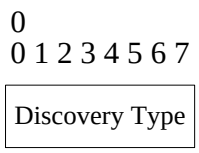


附图 34 Delete Station 消息要素格式

Type：Delete Station 为 18
Length：>= 8
Radio ID：8 位值，表示无线电设备，它的值在 1 和 31 间。
Length：MAC Address 字段长度。支持[EUI-48]和[EUI-64]中规定的格式和长度。
MAC Address：该站的 MAC 地址。

4-6-21 发现类型

Discovery Type 消息要素由 WTP 用于简要说明，它是如何最终知道存在一个 AC，它正在向该 AC 发送 Discovery Request 消息。Discovery Type 消息要素格式如附图 35 所示。



附图 35 Discovery Type 消息要素格式

Type：Discovery Type 为 20
Length：1
Discovery Type：8 位值，指出 WTP 如何发现 AC。支持下述枚举值：

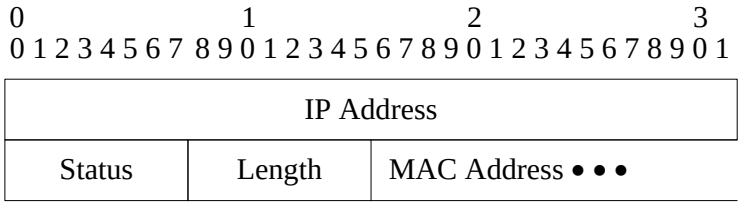
0 – 未知
1 – 静态配置
2 – DHCP
3 – DNS
4 – AC Referral(当或者通过 AC IPv4 List，或者通过 AC IPv6 List 消息要素配置 AC 时，使用。)

4-6-22 重复的 IPv4 地址

Duplicate IPv4 Address 消息要素由 WTP 用于通知 AC，该 WTP 已经检测到另一台 IP 设备，该 IP 设备使用的 IP 地址与此 WTP 目前正在使用的相同。

WTP 检测到重复的 IP 地址后，它**必须**发送这条(将状态设置为 1)消息要素。WTP 检测

到重复 IP 地址已经被清除后，它**必须**发送这条(将状态设置为 0)消息要素。Duplicate IPv4 Address 消息要素格式如附图 36 所示。



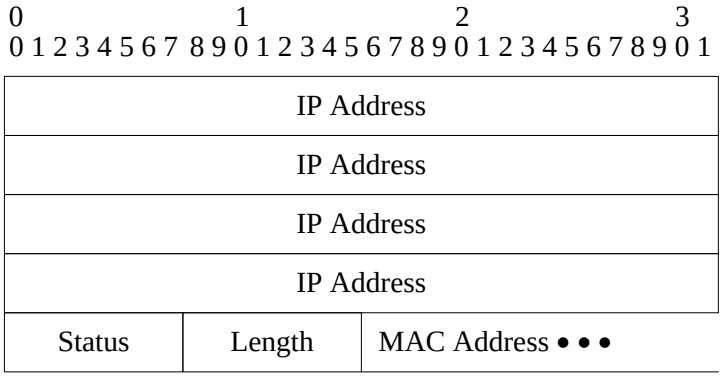
附图 36　Duplicate IPv4 Address 消息要素格式

Type：Duplicate IPv4 Address 为 21
Length：>= 12
IP Address：目前由该 WTP 使用的 IP 地址。
Status：该重复 IP 地址状态。当检测到重复地址时此值**必须**设置 1，清除重复地址后设置为 0。
Length：MAC Address 字段长度。支持[EUI-48]和[EUI-64]中规定的格式和长度。
MAC Address：违规设备的 MAC 地址。

4-6-23　重复的 IPv6 地址

Duplicate IPv6 Address 消息要素由 WTP 用于通知 AC，WTP 已经检测到另一台主机，该主机使用的 IP 地址与此 WTP 目前正在使用的相同。

WTP 检测到重复的 IP 地址后，它**必须**发送这条(将状态设置为 1)消息要素。WTP 检测到重复 IP 地址已经被清除后，它**必须**发送这条(将状态设置为 0)消息要素。Duplicate IPv6 Address 消息要素格式如附图 37 所示。

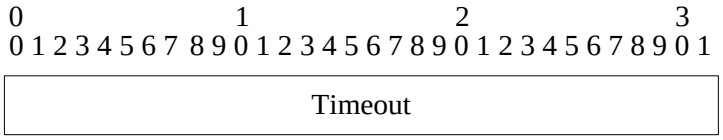


附图 37　Duplicate IPv6 Address 消息要素格式

Type：Duplicate IPv6 Address 为 22
Length：>= 24
IP Address：目前由该 WTP 使用的 IP 地址。
Status：重复 IP 地址状态。当检测到重复地址时此值**必须**设置 1，清除重复地址后设置为 0。
Length：MAC Address 字段长度。支持[EUI-48]和[EUI-64]中规定的格式和长度。
MAC Address：违规设备的 MAC 地址。

4-6-24　空闲超时

Idle Timeout 消息要素由 AC 发送给 WTP，向其提供 Idle Timeout 值，WTP 在它所有激活的站中**应当**强制执行此值。此值适用于在 WTP 上的所有无线电设备。Idle Timeout 消息要素格式如附图 38 所示。



附图 38　Idle Timeout 消息要素格式

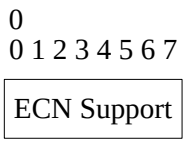
Type：Idle Timeout 为 23

Length：4

Timeout：目前的 Idle Timeout，单位为秒，由 WTP 强制执行。这个消息要素的默认值在第 4-7-8 节规定。

4-6-25　ECN 支持

ECN Support 消息要素由 WTP 和 AC 发送，指出它们支持 Explicit Congestion Notification (ECN)位，如[RFC3168]中定义的。ECN Support 消息要素格式如附图 39 所示。



附图 39　ECN Support 消息要素格式

Type：ECN Support 为 53

Length：1

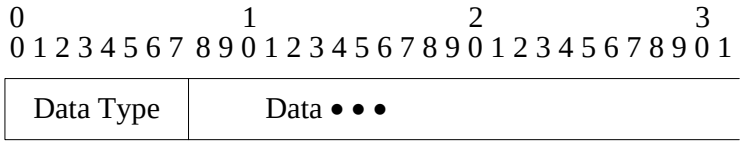
ECN Support：8 位值，表示发送方支持 ECN，如[RFC3168]中定义的。所有 CAPWAP 实现**必须**支持 Limited ECN Support 模式。如果 WTP 和 AC 通告，能够支持“Full 和 Limited ECN”，使用 Full ECN Support；否则，使用 Limited ECN Support。

0 - Limited ECN Support

1 – Full 和 Limited ECN Support

4-6-26　映像数据

Image Data 消息要素出现在 AC 发送的 Image Data Request 消息中，包括下述字段。Image Data 消息要素格式如附图 40 所示。



附图 40　Image Data 消息要素格式

Type：Image Data 为 24

Length：>= 1

Data Type：8 位值，表示映像 Data Type。支持下述枚举值：

1 – 包括映像数据。

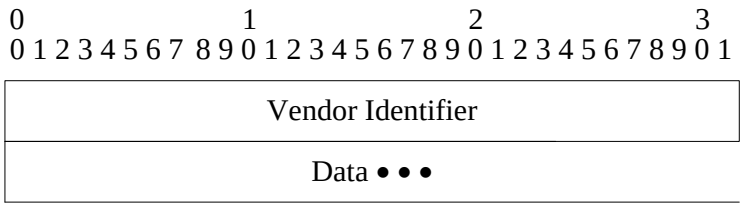
2 – 包括最后一个 Image Data Block (EOF)。

5 – 发生错误，传送被终止。

Data：Image Data 字段最多包括 1024 个字符，它的长度根据这个消息要素的长度字段推出。如果发送的是最后一个块，Data Type 字段设置为 2。通过将 Data Type 字段设置为 5，AC 可以选择终止数据传送。如 Data Type 字段是 5，Value 字段长度为 0。

4-6-27 映像标识符

Image Identifier 消息要素由 AC 发送给 WTP，指出预期将在 WTP 上运行的激活软件版本。为了向 AC 请求特定软件版本，WTP 发送 Image Identifier 消息要素。实际下载处理在第 9-1 节介绍。该值是可变长度 UTF-8 编码串[RFC3629]，它不以 0 结束。Image Identifier 消息要素格式如附图 41 所示。



附图 41 Image Identifier 消息要素格式

Type：Image Identifier 为 25

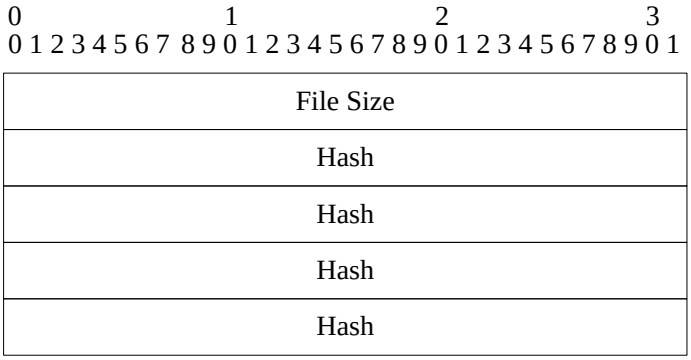
Length：>= 5

Vendor Identifier：32 位值，包括 IANA 分配的“SMI Network Management Private Enterprise Codes”。

Data：可变长度 UTF-8 编码串[RFC3629]，包括在 WTP 上运行的固件标识符，其长度必须不能超过 1024 个八位位组。这个字段的长度根据这个消息要素的长度字段推出。

4-6-28 映像信息

Image Information 消息要素出现在由 AC 发送给 WTP 的 Image Data Response 消息中，包含下述字段。Image Information 消息要素格式如附图 42 所示。



附图 42 Image Information 消息要素格式

Type：Image Information 为 26

Length：20

File Size：32 位值，包括文件的长度，单位为字节，它将由 AC 传送给 WTP。

Hash：16 字节 MD5 映像哈希函数，使用[RFC1321]中定义的程序。

4-6-29　启动下载

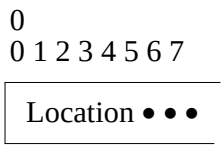
Initiate Download 消息要素由 WTP 用于通知 AC，AC 应当发起固件更新。AC 随后发送 Image Data Request 消息，该消息包括 Image Data 消息要素。这个消息要素不包括任何数据。

Type：Initiate Download 为 27

Length：0

4-6-30　位置数据

Location Data 消息要素是字节长度可变 UTF-8 编码串[RFC3629]，包含用户定义的位置信息(如，“Next to Fridge”)。这个信息由网络管理员配置，用于确定 WTP 的位置。这个串不以 0 结束。Location Data 消息要素格式如附图 43 所示。



附图 43　Location Data 消息要素格式

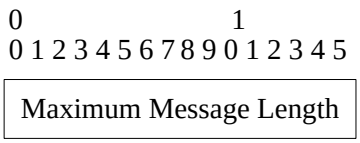
Type：Location Data 为 28

Length：>= 1

Location：包含此 WTP 位置的 UTF-8 编码串[RFC3629]，这个编码串不以 0 结束。它的最大长度必须不能超过 1024。

4-6-31　最大消息长度

Maximum Message Length 消息要素由 WTP 包括在 Join Request 消息中，用于告诉 AC 该 WTP 支持的最大 CAPWAP 消息长度。也可以选择由 AC 将 Maximum Message Length 消息要素包括在 Join Response 消息中，用于告诉 WTP 该 AC 支持的最大 CAPWAP 消息长度。Maximum Message Length 消息要素格式如附图 44 所示。



附图 44　Maximum Message Length 消息要素格式

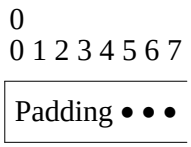
Type：Maximum Message Length 为 29

Length：2

Maximum Message Length：16 位无符号整数，包括最大消息长度。

4-6-32　MTU 发现填充

MTU Discovery Padding 消息要素用作填充，执行 MTU 发现，必须包含值为 0xFF，长度任意的八位位组。MTU Discovery Padding 消息要素格式如附图 45 所示。

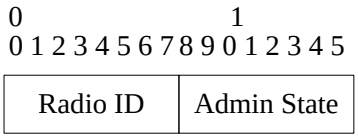


附图 45　MTU Discovery Padding 消息要素格式

Type：MTU Discovery Padding 为 52
Length：可变
Pad：可变长度填充，用 0xFF 值填充。

4-6-33　无线电设备管理状态

Radio Administrative State 消息要素用于传递特定无线电设备的状态。该信息要素由 AC 发送，用于改变 WTP 状态。WTP 保存该值，以便确保 WTP 重置后仍维持不变。在配置阶段期间，WTP 在 Configuration Status Request 消息中传递这个消息要素，以便确保 AC 掌握该 WTP 无线电设备目前管理状态设置。Radio Administrative State 消息要素格式如附图 46 所示。

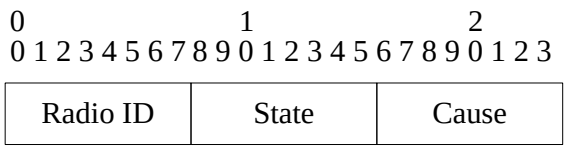


附图 46　Radio Administrative State 消息要素格式

Type：Radio Administrative State 为 31
Length：2
Radio ID：8 位值，表示配置的无线电设备，它的值在 1 和 31 之间。Radio ID 字段也**可以**包括 0xff 值，用于标识 WTP。如果 AC 希望改变 WTP 的管理状态，AC 在 Radio ID 字段中包括 0xff。
Admin State：8 为值，表示无线电设备的管理状态。Admin State 字段的默认值在第 4-8-1 节中列出。支持下述枚举值：
0 – 保留
1 – 开启
2 – 关闭

4-6-34　无线电设备运行状态

Radio Operational State 消息要素由 WTP 发送给 AC，传递无线电设备的运行状态。如果经 Radio Administrative State 消息要素，WTP 被要求改变它的无线电设备的状态但是 WTP 没能执行该请求，WTP 将 Radio Operational State 消息要素放在 Configuration Update Response 消息中。当 WTP 无线电设备状态意外改变时，这个消息要素被包括在 Change State Event 消息中。当硬件发生故障时会出现这种情况。注意，WTP 上不保存运行状态设置，因此，WTP 重置后不能维持不变。Radio Operational State 消息要素的值包含 3 个字段，其格式如附图 47 所示。



附图 47　Radio Operational State 消息要素格式

Type：Radio Operational State 为 32

Length：3

Radio ID：Radio Identifier 指 WTP 上的接口前缀，它的值在 1 和 31 之间。0xFF 无效，因为不可能改变 WTP 的运行状态。

State：8 位 Boolean 值，表示无线电设备状态。支持下述枚举值：

0 - 保留

1 - 开启

2 - 关闭

Cause：当无线电设备不可使用时，原因字段包含该无线电设备不能工作的原因。支持下述枚举值：

0 - 正常

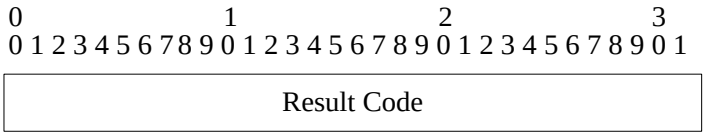
1 - 无线电设备故障

2 - 软件故障

3 - 管理设置

4-6-35 结果代码

Result Code 消息要素是 32 位整数值，包括 Request 消息结果，该 Request 消息对应 Response 消息中含有的序列号。Result Code 消息要素格式如附图 48 所示。



附图 48 Result Code 消息要素格式

Type：Result Code 为 33

Length：4

Result Code：定义有下述枚举值：

0 Success

1 Failure (必须有 AC List 消息要素)

2 Success (检测到 NAT)

3 Join Failure (未规定)

4 Join Failure (资源枯竭)

5 Join Failure (来源不明)

6 Join Failure (不正确的数据)

7 Join Failure (Session ID 已经在使用)

8 Join Failure (WTP 硬件不支持)

9 Join Failure (绑定不支持)

10 Reset Failure (不能重新设置)

11 Reset Failure (固件写错误)

12 Configuration Failure (不能使用请求的配置 - 无论提供什么服务)

13 Configuration Failure (不能使用请求的配置 - 不提供服务)

14 Image Data Error (不合法的校验和)

15 Image Data Error (不合法的数据长度)

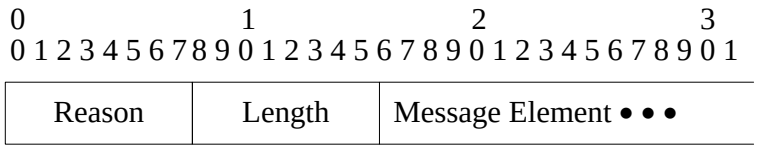
16 Image Data Error (其他错误)

17 Image Data Error (映像已经存在)

18 Message Unexpected (在目前状态不合法)
19 Message Unexpected (无法识别的请求)
20 Failure - 缺少强制性消息要素
21 Failure - 无法识别的消息要素
22 Data Transfer Error (没有信息传送)

4-6-36 返回的消息要素

Returned Message Element 由 WTP 在 Change State Event Request 消息中发送，用于通知 AC 它不能在本地使用 Configuration Status Response 中的哪些消息要素。Returned Message Element 消息要素包括结果编码，该结果编码指出配置不能使用的原因。Returned Message Element 消息要素封装出故障的消息要素。Returned Message Element 消息要素格式如附图 49 所示。

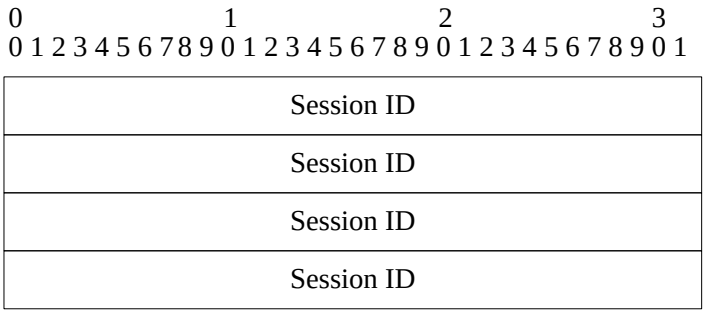


附图 49 Returned Message Element 消息要素格式

Type：Returned Message Element 为 34
Length：>= 6
Reason：在违规消息要素中的配置不能由 WTP 应用的原因。支持下述枚举值：
0 - 保留
1 - 未知的消息要素
2 - 不支持的消息要素
3 - 未知的消息要素值
4 - 不支持的消息要素值
Length：Message Element 字段长度，它**必须不能**超过 255 个八位位组。
Message Element：Message Element 字段封装由 AC 在 Configuration Status Response 消息中发送的消息要素(该消息要素引发错误)。

4-6-37 会话 ID

Session ID 消息要素值包含随机产生的无符号 128 位整数。Session ID 消息要素格式如附图 50 所示。



附图 50 Session ID 消息要素格式

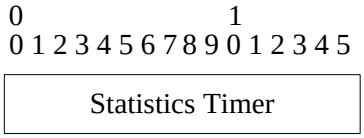
Type：Session ID 为 35

Length：16

Session ID：128 位无符号整数，用作随机会话标识符。

4-6-38 统计量计时器

Statistics Timer 消息要素值由 AC 用于告诉 WTP，WTP 将以此频次收到的它盼望的最新统计数据。Statistics Timer 消息要素格式如附图 51 所示。



附图 51 Statistics Timer 消息要素格式

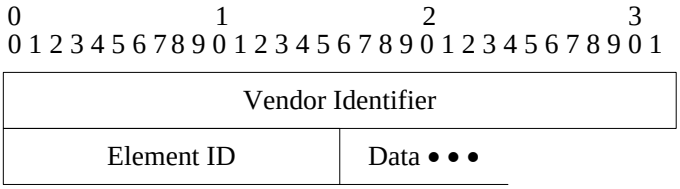
Type：Statistics Timer 为 36

Length：2

Statistics Timer：16 位无符号整数，指出时间，单位为秒。这个计时器的默认值在第 4-7-14 节规定。

4-6-39 特定供应商净荷

Vendor Specific Payload 消息要素用于在 WTP 和 AC 间传递特定供应商信息。Vendor Specific Payload 消息要素**可以**出现在任何 CAPWAP 消息中。WTP 和 AC 间特定供应商数据交换**必须不能**修改基本 CAPWAP 协议和状态机的行为。Vendor Specific Payload 消息要素格式如附图 52 所示。



附图 52 Vendor Specific Payload 消息要素格式

Type：Vendor Specific Payload 为 37

Length：>= 7

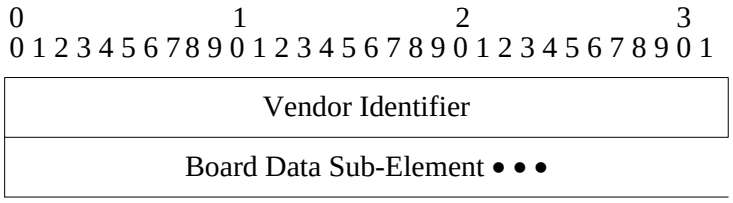
Vendor Identifier：32 位值，包括 IANA 分配的“SMI Network Management Private Enterprise Codes” [RFC3232]。

Element ID：16 位 Element Identifier，由供应商管理。

Data：长度可变特定供应商信息，其内容和格式是专有的，基于 Element ID 字段理解。这个字段**必须不能**超过 2048 个八位位组。

4-6-40 WTP 主板(Board)数据

WTP Board Data 消息要素由 WTP 发送给 AC，包括目前硬件信息。WTP Board Data 消息要素格式如附图 53 所示。



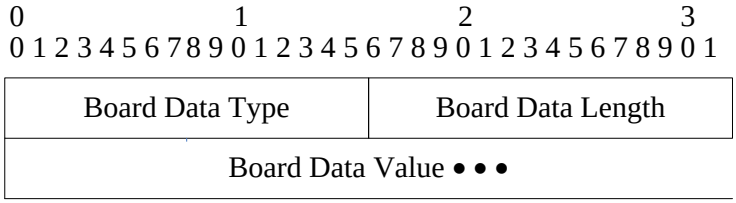
附图 53　　WTP Board Data 消息要素格式

Type：WTP Board Data 为 38

Length：>=14

Vendor Identifier：32 为值，包含 IANA 分配的“SMI Network Management Private Enterprise Codes”，标识 WTP 硬件制造商。Vendor Identifier 字段**必须不能**设置为 0。

Board Data Sub-Element：WTP Board Data 消息要素包括多个 Board Data 子要素，其中一些是强制的，一些是可选的，如下所示。Board Data Type 值不能由供应商扩展，因此不与 Vendor Identifier 字段配对。Board Data 子要素格式如附图 54 所示。



附图 54　　Board Data 子要素格式

Board Data Type：Board Data Type 字段标识正在被编码的数据。CAPWAP 协议定义下述值，这些类型中的每一种指出它们是必须存在还是可以选择：

0 - WTP Model Number：WTP Model Number **必须**包括在 WTP Board Data 消息要素中。

1 - WTP Serial Number：WTP Serial Number **必须**包括在 WTP Board Data 消息要素中。

2 - Board ID：硬件标识符，它**可以**包括在 WTP Board Data 消息要素中。

3 - Board Revision：主板的修订版本号，它**可以**包括在 WTP Board Data 消息要素中。

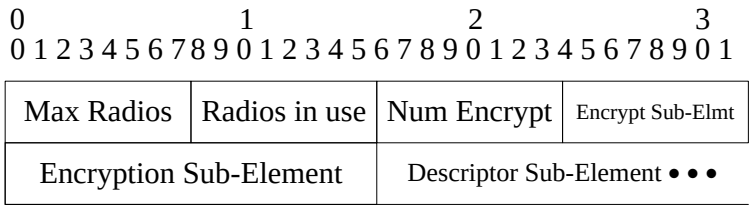
4 - Base MAC Address：WTP 的 Base MAC 地址，**可以**将其分配给主以太网接口。

Board Data Length：Board Data Value 字段中数据长度，其长度**必须不能**超过 1024 个八位位组。

Board Data Value：与这个 Board Data 子要素的 Board Data Type 字段关联的数据

4-6-41　WTP 描述符

WTP Descriptor 消息要素由 WTP 用于传递它目前的硬件和软件(固件)配置。WTP Descriptor 消息要素格式如附图 55 所示。



附图 55　　WTP Descriptor 消息要素格式

Type：WTP Descriptor 为 39

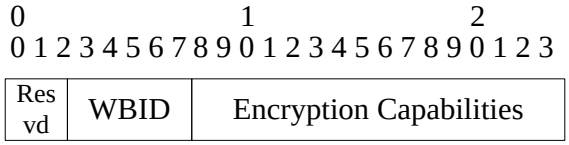
Length：>= 33

Max Radios：8 位值，表示 WTP 支持的无线电设备数目(这里，由 Radio ID 字段定义每一个无线电设备)。

Radios in use：8 位值，表示 WTP 中使用的无线电设备数目。

Num Encrypt：跟在这个字段后的 3 字节加密子要素数目。Num Encrypt 字段值**必须**在 1 和 255 间。

Encryption Sub-Element：WTP Descriptor 消息要素**必须**包含至少一个 Encryption 子要素。WTP 支持的每个绑定有一个子要素。Encryption 子要素格式如附图 56 所示。



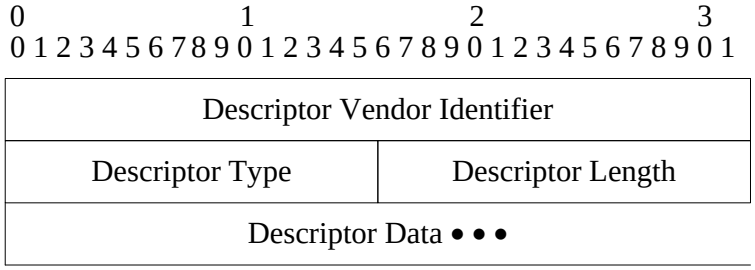
附图 56　Encryption 子要素格式

Resvd：3 位字段，保留将来使用。遵循这个协议的所有实现**必须**将由该实现支持的协议版本中保留的任何位设置为 0。接收方**必须**忽略不是为它们支持的协议版本定义的所有位。

WBID：5 位字段，它是无线绑定标识符。此标识符指出与该无线电设备关联的无线分组类型。本规范定义的 WBIDs 可在第 4-3 节找到。

Encryption Capabilities：16 位字段，由 WTP 用于向 AC 传递它的能力。没有任何加密能力的 WTP 将这个字段设置为 0。Encryption Capabilities 字段更进一步的详细介绍请参阅具体的无线绑定。

Descriptor Sub-Element：WTP Descriptor 消息要素包含多个 Descriptor 子要素，其中一些是强制性的，一些是可选的，如下所示。Descriptor 子要素格式如附图 57 所示。



附图 57　Descriptor 子要素格式

Descriptor Vendor Identifier：32 位值，包括 IANA 分配的“SMI Network Management Private Enterprise Codes”。

Descriptor Type：Descriptor Type 字段标识正在被编码的数据。数据格式是供应商特定的，采用 UTF-8 格式[RFC3629]编码。CAPWAP 协议定义下述值，这些类型中的每一种指出它们是必须存在还是可以选择。下面列出的值与 Descriptor Vendor Identifier 字段一起使用，该字段的值**必须**被设置为 0。Descriptor Type 字段，结合设置为非 0 值的 Descriptor Vendor Identifier，允许供应商使用私有命名空间。

0 - Hardware Version：WTP 硬件版本号**必须**存在。

1 - Active Software Version：WTP 运行的软件版本号**必须**存在。

2 - Boot Version：WTP 引导加载程序版本号**必须**存在。

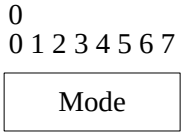
3 - Other Software Version：WTP 非运行软件(固件)版本号**可以**存在。这个类型用于传递可替代的软件版本，这些软件版本可以在 WTP 的非易失性存储器上获得。

Descriptor Length：Descriptor Data 字段的供应商特定编码长度，这个长度**必须不能**超过 1024 个八位位组。

Descriptor Data：WTP 的供应商特定数据信息，采用 UTF-8 格式[RFC3629]编码。

4-6-42 WTP 回退

WTP Fallback 消息要素由 AC 发送给 WTP，用于当 WTP 检测到它的首选 AC(WTP 目前没有连接到该 AC)时，开启或关闭自动 CAPWAP 回退。WTP Fallback 消息要素格式如附图 58 所示。



附图 58 WTP Fallback 消息要素格式

Type：WTP Fallback 为 40

Length：1

Mode：8 位值，指出 WTP 上自动 CAPWAP 回退状态。开启时，如果 WTP 检测到它的主 AC 可用，并且 WTP 没有连接到主 AC，WTP **应当**自动断开它目前连接的 AC 并重新连接到它的主 AC。关闭时，WTP 仅能通过人工干预重新连接到它的主 AC(例如，通过 Reset Request 消息)。这个字段默认值在第 4-8-9 节规定。支持下述枚举值：

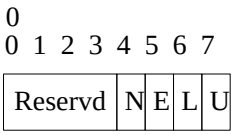
0 - 保留

1 - 开启

2 - 关闭

4-6-43 WTP 帧隧道模式

WTP Frame Tunnel Mode 消息要素使 WTP 能够告诉 AC，它支持的隧道化运行模式。通告支持所有类型的 WTP 使 AC 能够根据它的本地策略选择将使用哪种类型。WTP Frame Tunnel Mode 消息要素格式如附图 59 所示。



附图 59 WTP Frame Tunnel Mode 消息要素格式

Type：WTP Frame Tunnel Mode 为 41

Length：1

Reservd：一组保留位留作将来使用。所有遵循这个协议的实现**必须**将由该实现支持的协议版本中保留的任何位设置为 0。接收方**必须**忽略不是为它们支持的协议版本定义的所有位。

N：Native Frame Tunnel 模式要求 WTP 和 AC 将所有用户净荷封装为本地无线帧，如无线绑定定义的(相关举例参阅第 4-4 节)。

E：802.3 Frame Tunnel Mode 要求 WTP 和 AC 将所有用户净荷封装为本地 IEEE 802.3 帧(参

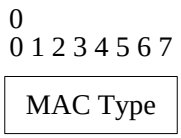
阅第 4-4 节)。所有用户流量被隧道化给 AC。当 WTP MAC Type 设置为 Split MAC 时，**必须不能**使用这个值。

L：当使用 Local Bridging 时，WTP 不将传给 AC 的用户流量隧道化；所有用户流量在本地桥接。当 WTP MAC Type 设置为 Split MAC 时，**必须不能**使用这个值。

R：此位留作将来使用。所有遵循这个协议的实现**必须**将由该实现支持的协议版本中保留的任何位设置为 0。接收方**必须**忽略不是为它们支持的协议版本定义的所有位。

4-6-44　WTP MAC 类型

WTP MAC Type 消息要素使 WTP 能够将它的运行模式告诉 AC。通告支持两种模式的 WTP 使 AC 能够根据本地策略选择使用的模式。WTP MAC Type 消息要素格式如附图 60 所示。



附图 60　WTP MAC Type 消息要素格式

Type：WTP MAC Type 为 44

Length：1

MAC Type：WTP 支持的 MAC 运行模式。支持下述枚举值：

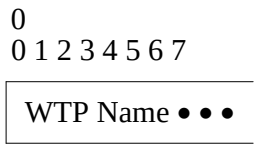
0 - Local MAC：Local MAC 是默认模式，所有 WTPs **必须**支持。开启隧道化时(参阅第 4-6-43 节)，封装的帧**必须**采用 802.3 格式(参阅第 4-4-2 节)，无线管理或控制帧除外，这样的帧**可以**采用它自己的本地格式。任何 CAPWAP 绑定都需要规定管理和控制无线帧的格式。

1 - Split MAC：支持 Split MAC 是可选的，允许 AC 接收和处理本地无线帧。

2 - Both：WTP 能够支持 Local MAC 和 Split MAC。

4-6-45　WTP 名称

WTP Name 消息要素是可变长度 UTF-8 编码字节串[RFC3629]。该串不能以 0 终止。WTP Name 消息要素格式如附图 61 所示。



附图 61　WTP Name 消息要素格式

Type：WTP Name 为 45

Length：>= 1

WTP Name：不以 0 终止的 UTF-8 编码串[RFC3629]，包含 WTP 名称，它的最大长度**必须不能**超过 512 字节。

4-6-46　WTP 无线电设备统计量

WTP Radio Statistics 消息要素由 WTP 发送给 AC，传递关于无线电设备行为的统计数据，以及重新设置 WTP 无线电设备的原因。WTP 上的这些计数器绝不复位，因此，当达到

最大值时将翻转到 0。WTP Radio Statistics 消息要素格式如附图 62 所示。

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Radio ID	Last Fail Type	Reset Count
SW Failure Count		HW Failure Count
Other Failure Count		Unknown Failure Count
Config Update Count		Channel Change Count
Band Change Count		Current Noise Floor

附图 62　WTP Radio Statistics 消息要素格式

Type：WTP Radio Statistics 为 47
Length：20
Radio ID：应用这些统计量的无线电设备的无线电设备 ID，它的值在 1 和 31 间。
Last Failure Type：最后的 WTP 故障。支持下述枚举值：

0 - 不支持的统计量
1 - 软件故障
2 - 硬件故障
3 - 其他故障
255 - 未知(例如，WTP 不跟踪信息)

Reset Count：无线电设备被复位的次数。
SW Failure Count：由于相关软件原因，无线电设备出故障的次数。
HW Failure Count：由于相关硬件原因，无线电设备出故障的次数。
Other Failure Count：由于除软件或硬件故障以外的已知原因，无线电设备出故障的次数。
Unknown Failure Count：未知原因造成的无线电设备故障次数。
Config Update Count：无线电设备配置升级次数。
Channel Change Count：无线电设备信道改变次数。
Band Change Count：无线电设备频率段改变次数。
Current Noise Floor：有符号整数，指出无线电设备接收机的本底噪声，单位为 dBm。

4-6-47　WTP 重启统计量

WTP Reboot Statistics 消息要素由 WTP 发送给 AC，传递 WTP 发生重新启动的原因。WTP 上的这些计数器绝不复位，因此，当达到最大值时将翻转到 0。WTP Reboot Statistics 消息要素格式如附图 63 所示。

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Reboot Count	AC Initiated Count
Link Failure Count	SW Failure Count
HW Failure Count	Other Failure Count
Unknown Failure Count	Last Failure Type

附图 63　WTP Reboot Statistics 消息要素格式

Type：WTP Reboot Statistics 为 48

Length：15

Reboot Count：由于 WTP 崩溃导致重启的次数。值为 65535 意味着这个信息在 WTP 上不能使用。

AC Initiated Count：应 CAPWAP 协议消息要求发生的重启次数，诸如改变配置(它要求重启)或显式 CAPWAP 协议复位要求。值为 65535 意味着这个信息在 WTP 上不能使用。

Link Failure Count：由于链路故障，与 AC 的 CAPWAP 协议连接失败的次数。

SW Failure Count：由于相关软件原因，与 AC 的 CAPWAP 协议连接失败的次数。

HW Failure Count：由于相关硬件原因，与 AC 的 CAPWAP 协议连接失败的次数。

Other Failure Count：除了 AC 启动、链路、软件或硬件故障以外，由于已知原因，与 AC 的 CAPWAP 协议连接失败的次数。

Unknown Failure Count：由于未知原因，与 AC 的 CAPWAP 协议连接失败的次数。

Last Failure Type：最新 WTP 故障的故障类型。支持下述枚举值：

0 - 不支持

1 - AC 启动(参阅第 9-2 节)

2 - 链路故障

3 - 软件故障

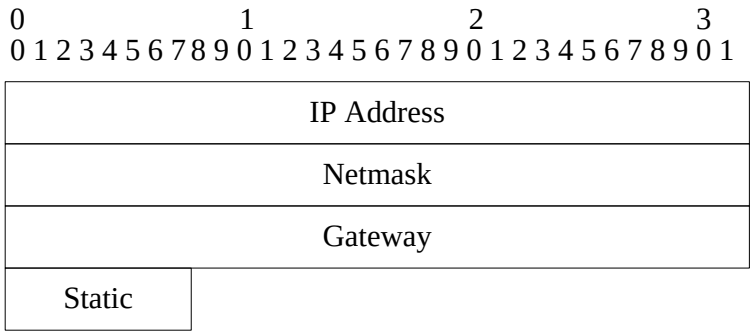
4 - 硬件故障

5 - 其他故障

255 - 未知(例如，WTP 不跟踪信息)

4-6-48 WTP 静态 IP 地址信息

WTP Static IP Address Information 消息要素由 AC 用于在 WTP 上配置或删除先前配置的静态 IP 地址。IPv6 WTP 预期使用动态地址。WTP Static IP Address Information 消息要素格式如附图 64 所示。



附图 64 WTP Static IP Address Information 消息要素格式

Type：WTP Static IP Address Information 为 49

Length：13

IP Address：分配给 WTP 的 IP 地址。仅当静态字段设置为 1 时这个字段有效。

Netmask：IP Netmask。仅当静态字段设置为 1 时这个字段有效。

Gateway：网关的 IP 地址。仅当静态字段设置为 1 时这个字段有效。

Static：8 位 Boolean 值，说明是否 WTP 应当使用静态 IP 地址。取 0 值表示关闭静态 IP 地址，取 1 值表示开启静态 IP 地址。

4-7 CAPWAP 协议计时器

本节介绍 CAPWAP 计时器定义。

4-7-1 ChangeStatePendingTimer

最长时间，单位为秒，成功发送 Configuration Status Response 消息后，AC 等待来自 WTP 的 Change State Event Request 时间。

默认：25 秒

4-7-2 DataChannelKeepAlive

DataChannelKeepAlive 计时器由 WTP 用于确定它下一次必须发送 Data Channel Keep-Alive 的时机，单位为秒。

默认：30 秒

4-7-3 DataChannelDeadInterval

最短时间，单位为秒，在可以认为 Data Channel Keep-Alive 分组的目的地无效前，如果没有收到 Data Channel Keep-Alive 分组，WTP **必须**等待这个时间间隔。这个计时器的值**不能**小于 2 × DataChannelKeepAlive 秒，也**不能**大于 240 秒。

默认：60 秒

4-7-4 DataCheckTimer

AC 等待 Data Channel Keep Alive 时间，单位为秒，它是 CAPWAP 状态机的 Data Check 状态要求的。如果在转换到下一个状态前这个计时器到期，AC 复位该状态机。

默认：30 秒

4-7-5 DiscoveryInterval

最短时间，单位为秒，在收到 Discovery Response 消息后，启动 DTLS 握手前，WTP **必须**等待的时间间隔。

默认：5 秒

4-7-6 DTLSSessionDelete

最短时间，单位为秒，WTP **必须**等待 DTLS 会话删除的时间。

默认：5 秒

4-7-7 EchoInterval

最短时间，单位为秒，发送给 AC(WTP 已经加入该 AC)的多个 Echo Request 消息间的时间间隔。

默认：30 秒

4-7-8 IdleTimeout

默认的 Idle Timeout 为 300 秒。

4-7-9 ImageDataStartTimer

WTP 等待它的对端发送 Image Data Request 的时间，单位为秒。

默认：30 秒

4-7-10 MaxDiscoveryInterval

发送多个 Discovery Request 消息时允许的最大间隔时间，单位为秒。这个值**不能**小于 2 秒，也**不能**大于 180 秒。

默认：20 秒

4-7-11 ReportInterval

WTP 发送多个通知 AC 加密错误的 Decryption Error 消息要素时，WTP 使用 ReportInterval 来确定两次发送间的时间间隔，单位为秒。

默认 Report Interval 为 120 秒。

4-7-12 RetransmitInterval

最短时间，单位为秒，过此时间间隔后将重传没有得到确认的 CAPWAP 分组。

默认：3 秒

4-7-13 SilentInterval

对于 WTP，这是最短时间，单位为秒，WTP **可以**再次发送 Discovery Request 消息或尝试建立 DTLS 会话前，WTP **必须**等待这个时间间隔。对于 AC，这是最短时间，单位为秒，在此期间 AC **应当**忽略从处于 Sulking 状态的 WTP 收到的所有 CAPWAP 和 DTLS 分组。

默认：30 秒

4-7-14 StatisticsTimer

在 WTP 发送多个给 AC 的、传递它的统计数据的 WTP Events Requests 时，WTP 使用 The StatisticsTimer 来确定两次发送间的时间间隔，单位为秒。

默认：120 秒。

4-7-15 WaitDTLS

最长时间，单位为秒，没有收到来自 AC 的 DTLS Handshake 消息，WTP **必须**等待这个时间。这个计时器**必须**大于 30 秒。

默认：60

4-7-16 WaitJoin

最长时间，单位为秒，建立 DTLS 会话后，直到 AC 收到来自 WTP 的 Join Request 前，AC 将等待这个时间。这个计时器**必须**大于 20 秒。

默认：60 秒

4-8 CAPWAP 协议变量

这一节定义 CAPWAP 协议变量，协议变量用于各种协议功能。有些变量是可配置的，而其他的是计数器或有固定值。对于非计数器相关变量，规定默认值。然而，如果 WTP 的变量配置被 AC 显式重写，WTP **必须**保存新值。

4-8-1 AdminState

开启默认 Administrative State 值(1)。

4-8-2 DiscoveryCount

由 WTP 发送给单个 AC 的 Discovery Request 消息数目。这是单调增加的计数器。

4-8-3 FailedDTLSAuthFailCount

由于认证故障，DTLS 会话建立尝试失败的次数。

4-8-4 FailedDTLSSessionCount

DTLS 会话建立尝试失败的次数。

4-8-5 MaxDiscoveries

WTP 启动后，Discovery Request 消息将要发送的最大次数。

默认：10

4-8-6 MaxFailedDTLSSessionRetry

CAPWAP 设备进入静默期前，进行 DTLS 会话建立尝试的最大次数。

默认：3

4-8-7 MaxRetransmit

链路层认为对端失效前，重传给定 CAPWAP 分组的最大次数。

4-8-8 RetransmitCount

重传给定 CAPWAP 分组的次数。这是单调增加的计数器。

4-8-9 WTPFallBack

开启默认 WTP Fallback 值(1)。

4-9 WTP 保存的变量

除了在第 4-8 节定义的值以外，下述值**应当**保存在 WTP 非易失性存储器中。CAPWAP 无线绑定**可以**定义补充值，这些值**应当**保存在 WTP 上。

4-9-1 AdminRebootCount

因管理原因重新启动 WTP 的次数，在第 4-6-47 节定义。

4-9-2 FrameEncapType

对于支持多 Frame Encapsulation Types 的 WTPs，保存 AC 配置的值很有必要。Frame Encapsulation Type 在第 4-6-43 节定义。

4-9-3 LastRebootReason

WTP 最后一次重新启动的原因，在第 4-6-47 节定义。

4-9-4 MacType

对于支持多 MAC-Types 的 WTPs，保存 AC 配置的值很有必要。MAC-Type 在第 4-6-44 节定义。

4-9-5 PreferredACs

用索引首选的 ACs，在第 4-6-5 节定义。

4-9-6 RebootCount

WTP 重新启动的次数，在第 4-6-47 节定义。

4-9-7 Static IP Address

分配给 WTP 的静态 IP 地址，如 WTP Static IP address Information 消息要素配置的(参阅第 4-6-48 节)。

4-9-8 WTPLinkFailureCount

链接到 AC 失败的次数，参阅第 4-6-47 节。

4-9-9 WTPLocation

WTP Location，在第 4-6-30 节定义。

4-9-10 WTPName

WTP Name，在第 4-6-45 节定义。

第 5 章 CAPWAP 发现操作

Discovery 消息由 WTP 用于确定哪一个 ACs 能够提供服务，以及确定 ACs 的能力和负载。

5-1 发现请求消息

Discovery Request 消息由 WTP 用于在网络中自动发现潜在的可用 ACs。Discovery Request 消息向 ACs 提供 WTP 的主要能力。WTP 必须与 ACs 交换这个信息，以确保后续的交换符合 WTP 的基本特性。

在 WTP 首次出现或被(重新)初始化后，WTP **必须**在 Discover 状态，等待短于 MaxDiscoveryInterval 的随机延时后，发送 Discovery Request 消息。WTP 发送 Discovery Request 消息**必须**不能超过 MaxDiscoveries 次，在两个连续的消息间等待短于 MaxDiscoveryInterval 的随机延时时间。

这是为了防止出现 WTP Discovery Request 消息爆炸。当许多 WTPs 同时启动时会出现这种情况。

如果发送最大次数的 Discovery Request 消息后，没有收到 Discovery Response 消息，WTP 进入 Sulking 状态，并**必须**等待等于 SilentInterval 的时间间隔才能继续发送 Discovery Request 消息。

一旦收到 Discovery Request 消息，AC 用 Discovery Response 消息响应，Discovery Response 消息发送到所接收 Discovery Request 消息源地址中的地址。一旦收到 Discovery Response，如果 WTP 决定与作出响应的 AC 建立会话，它**应当**执行 MTU 发现，使用在第 3-5 节描述的流程。

当与 WTP 的会话已经激活时，AC 可能收到明文 Discovery Request 消息。如果 WTP 重新启动，这是最可能出现的情况，可能的原因是软件或电源故障，但也可能因 DoS 攻击引起。在这些情况，**必须不能**清除任何 WTP 状态，包括状态机实例， 直到另一个 DTLS 会

话成功建立，且经过 DTLSSessionEstablished DTLS 通知告知(参阅第 2-3-2-2 节)。

在 Discovery Request 消息中包括绑定的特定 WTP Radio Information 消息要素(参阅第 2-1 节)，该消息要素通告 WTP 支持一个或多个 CAPWAP 绑定。

Discovery Request 消息由 WTP，在 Discovery 状态期间发送。AC 不发送这条消息。

在 Discovery Request 消息中**必须**包括下述消息要素：

- Discovery Type，参阅第 4-6-21 节
- WTP Board Data，参阅第 4-6-40 节
- WTP Descriptor，参阅第 4-6-41 节
- WTP Frame Tunnel Mode，参阅第 4-6-43 节
- WTP MAC Type，参阅第 4-6-44 节
- WTP 支持的 WTP Radio Information 消息要素；这些 WTP Radio Information 消息要素由各个链路层 CAPWAP Binding Protocols 定义(参阅第 2-1 节)。

在 Discovery Request 消息中**可以**包括下述消息要素：

- MTU Discovery Padding，参阅第 4-6-32 节
- Vendor Specific Payload，参阅第 4-6-39

5-2 发现响应消息

Discovery Response 消息提供的机制用于 AC 向需要的 WTPs 通告它的服务。

WTP 收到 Discovery Response 消息时，为了接收补充的 Discovery Response 消息，它**必须**等待不短于 DiscoveryInterval 的时间间隔。DiscoveryInterval 到期，WTP 进入 DTLS-Init 状态，选择发送了 Discovery Response 消息的 ACs 中的一个，并发送 DTLS Handshake 给该 AC。

在 Discovery Request 消息中包括一个或多个特别绑定的 WTP Radio Information 消息要素(参阅第 2-1 节)，以便通告 AC，WTP 支持哪些 CAPWAP 绑定。AC **可以**仅包括它与该 WTP 共享的那些绑定，AC 是通过在 Discovery Request 消息中收到的 WTP Radio Information 消息要素获知它与 WTP 共享这些绑定，或者 AC **可以**包括所有支持的绑定。WTP **可以**在它的 AC 决策流程中使用这些支持的绑定。注意，如果 WTP 所加入的 AC 不支持特定的 CAPWAP 绑定，WTP **必须不**提供该绑定的业务。

Discovery Response 消息由 AC，在 Idle 状态期间发送。WTP 不发送这条消息。

在 Discovery Response 消息中**必须**包括下述消息要素：

- AC Descriptor，参阅第 4-6-1 节
- AC Name，参阅第 4-6-1 节
- AC 支持的 WTP Radio Information 消息要素；这些 WTP Radio Information 消息要素由各个链路层 CAPWAP Binding Protocols 定义(参阅第 2-1 节)。
- 下述消息要素之一**必须**包括在 Discovery Response 消息中：
  * CAPWAP Control IPv4 Address，参阅第 4-6-9 节
  * CAPWAP Control IPv6 Address，参阅第 4-6-10 节

在 Discovery Response 消息中**可以**包括下述消息要素：

- Vendor Specific Payload，参阅第 4-6-39 节

5-3 主发现请求消息

Primary Discovery Request 消息由 WTP 发送，以便：

- 确定它的首选(或主)AC 是否可用，或者
- 执行 Path MTU Discovery(参阅第 3-5 节)。

当 WTP 有主 AC 配置，然而却被连接到另一个 AC 时，WTP 发送 Primary Discovery Request 消息。这通常由故障转换引起，它作为一种方法由 WTP 用作发现何时它的主 AC 变得可用。因为 WTP 仅有单个 CAPWAP 状态机实例，当处于 Run 状态时，WTP 发送 Primary Discovery Request。AC 不发送这条消息。

发送 Primary Discovery Request 消息不能太频繁，通常应当不超过发送 Echo Request 消息的频率。

一旦收到 Primary Discovery Request 消息，AC 用 Primary Discovery Response 消息响应，Primary Discovery Response 消息发送到所接收 Primary Discovery Request 消息源地址中的地址。

在 Primary Discovery Request 消息中**必须**包括下述消息要素

- Discovery Type，参阅第 4-6-21
- WTP Board Data，参阅第 4-6-40
- WTP Descriptor，参阅第 4-6-41
- Frame Tunnel Mode，参阅第 4-6-43
- WTP MAC Type，参阅第 4-6-44
- WTP 支持的 WTP Radio Information 消息要素；这些 WTP Radio Information 消息要素由各个链路层 CAPWAP Binding Protocols 定义(参阅第 2-1 节)。

在 Primary Discovery Request 消息中**可以**包括下述消息要素：

- MTU Discovery Padding，参阅第 4-6-32
- Vendor Specific Payload，参阅第 4-6-39

5-4　主发现响应消息

Primary Discovery Response 消息使 AC 能够向有需求的 WTPs 通告它的可用性和业务，而这些 WTPs 已经被配置为将该 AC 作为它的主 AC。

Primary Discovery Response 消息由 AC 在收到 Primary Discovery Request 消息后发送。

WTP 收到 Primary Discovery Response 消息后，根据 WTP 上的 WTP Fallback Status 消息要素配置，WTP 可以与它的主 AC 建立 CAPWAP 协议连接。

当处于 Run 状态时，AC 发送 Primary Discovery Response 消息。WTP 不发送这条消息。

Primary Discovery Response 消息中**必须**包括下述消息要素。

- AC Descriptor，参阅第 4-6-1
- AC Name，参阅第 4-6-4 节
- AC 支持的 WTP Radio Information 消息要素；这些 WTP Radio Information 消息要素由各个链路层 CAPWAP Binding Protocols 定义(参阅第 2-1 节)。

下述消息要素之一**必须**包括在 Primary Discovery Response 消息中：

- CAPWAP Control IPv4 Address，参阅第 4-6-9 节
- CAPWAP Control IPv6 Address，参阅第 4-6-10 节

在 Primary Discovery Response 消息中**可以**包括下述消息要素：

- Vendor Specific Payload，参阅第 4-6-39 节

第 6 章　CAPWAP 加入操作

Join Request 消息由 WTP 使用，是在与某个 AC 建立了 DTLS 连接后用于向那个 AC 请求服务。Join Response 消息由 AC 用于指出它将提供或不提供的服务。

6-1　加入请求

Join Request 由 WTP 用于向 AC 请求服务。如果 WTP 正在执行可选的 AC Discovery 流程(参阅第 3-3 节)，在 WTP 收到一个或多个 Discovery Response 消息后，加入流程发生。在 Discovery 流程期间，AC **可以**返回一个以上 CAPWAP Control IPv4 Address 消息要素或 CAPWAP Control IPv6 Address 消息要素。当返回一个以上这样的消息要素时，WTP **应当**通过选择当下服务的 WTPs 数量最少的接口(通过该消息要素的 WTP Count 字段获知)，执行“负载均衡”。然而，注意，也允许使用其他负载均衡算法。一旦 WTP 确定它的优先 AC，以及该 AC 上的相关接口，它建立 DTLS 会话，在此安全的控制通道上发送 Join Request。当 AC 收到 Join Request 消息，它用 Join Response 消息响应。

一旦完成 DTLS 握手，收到 DTLSEstablished 通知，WTP 发送 Join Request 消息给 AC。当 AC 获知 DTLS 会话建立后，它不清除 WaitDTLS 计时器，直到它收到 Join Request 消息，在那个时刻它发送 Join Response 消息给 WTP，指出成功或失败。

在 Join Request 中包括一个或多个 WTP Radio Information 消息要素(参阅第 2-1 节)，以便请求由 AC 提供的 CAPWAP bindings 服务。如果 AC 不支持包括的绑定，将导致 Join Response 失败。

如果 AC 拒绝 Join Request，它发送带失败指示的 Join Response 消息，通过 DTLSAbort 指令启动 DTLS 会话终止。

如果收到不合法的(例如，异常的)Join Request 消息，AC **必须**静默抛弃该消息。没有响应发送给 WTP。AC **应当**记录这一事件。

在 Join State 期间 WTP 发送 Join Request 消息。AC 不发送这条消息。

Join Request 消息中**必须**包括下述消息要素。

- Location Data，参阅第 4-6-30 节
- WTP Board Data，参阅第 4-6-40 节
- WTP Descriptor，参阅第 4-6-41 节
- WTP Name，参阅第 4-6-45 节
- Session ID，参阅第 4-6-37 节
- WTP Frame Tunnel Mode，参阅第 4-6-43 节
- WTP MAC Type，参阅第 4-6-44 节
- WTP 支持的 WTP Radio Information 消息要素；这些 WTP Radio Information 消息要素由各个链路层 CAPWAP Binding Protocols 定义(参阅第 2-1 节)。
- ECN Support，参阅第 4-6-25 节

在 Join Request 消息中**必须**至少包括下述消息要素之一。

- CAPWAP Local IPv4 Address，参阅第 4-6-11 节
- CAPWAP Local IPv6 Address，参阅第 4-6-12 节

在 Join Request 消息中**可以**包括下述消息要素。

- CAPWAP Transport Protocol，参阅第 4-6-14 节
- Maximum Message Length，参阅第 4-6-31 节
- WTP Reboot Statistics，参阅第 4-6-47 节
- Vendor Specific Payload，参阅第 4-6-39 节

6-2　加入响应

Join Response 消息由 AC 发送，用于通知 WTP 它能够并且愿意为该 WTP 提供服务。

收到 Join Response 消息，WTP 检验成功或失败。如果消息指出成功，WTP 清除该会话的 WaitDTLS 计时器，并进入 Configure 状态。

如果收到 Join Response 消息前 WaitDTLS 计时器到期，WTP **必须**终止握手，释放会话

状态，并启动 DTLSAbort 指令。

如果收到不合法(异常的)的 Join Response 消息，WTP **应当**记录详述错误的翔实消息。**必须**像对待 AC 不响应那样对待这个错误。WaitDTLS 计时器最终将到期，WTP **可以**尝试加入新的 AC(如果它是这样配置的)。

如果在 Join Request 消息中的 WTP Radio Information 消息要素之一(参阅第 2-1 节)要求支持 AC 不支持的 CAPWAP 绑定，AC 设置 Result Code 消息要素为“Binding Not Supported”。AC 包括 Image Identifier 消息要素，以便指出它希望 WTP 运行的软件版本。这条信息用于确定 WTP 是否**必须**改变它目前运行的固件映像或下载新的版本(参阅第 9-1-1 节)。

Join Response 消息由 AC 在 Join State 期间发送。WTP 不发送这条消息。

在 Join Response 消息中**必须**包括下述消息要素。

- Result Code，参阅第 4-6-35 节
- AC Descriptor，参阅第 4-6-1 节
- AC Name，参阅第 4-6-4 节
- AC 支持的 WTP Radio Information 消息要素；这些 WTP Radio Information 消息要素由各个链路层 CAPWAP Binding Protocols 定义(参阅第 2-1 节)。
- ECN Support，参阅第 4-6-25 节

在 Join Response 消息中**必须**包括下述消息要素之一：

- CAPWAP Control IPv4 Address，参阅第 4-6-9 节
- CAPWAP Control IPv6 Address，参阅第 4-6-10 节

在 Join Response 消息中**必须**包括下述消息要素之一：

- CAPWAP Local IPv4 Address，参阅第 4-6-11 节
- CAPWAP Local IPv6 Address，参阅第 4-6-12 节

在 Join Response 消息中**可以**包括下述消息要素。

- AC IPv4 List，参阅第 4-6-2 节
- AC IPv6 List，参阅第 4-6-3 节
- CAPWAP Transport Protocol，参阅第 4-6-14 节
- Image Identifier，参阅第 4-6-27 节
- Maximum Message Length，参阅第 4-6-31 节
- Vendor Specific Payload，参阅第 4-6-39 节

第7章　控制通道管理

Control Channel Management消息由WTP和AC使用，用于维持控制通信通道。CAPWAP Control消息，诸如从WTP发送到AC的WTP Event Request消息，向AC指出WTP是可以使用的。当不发送这样的控制消息时，Echo Request消息和Echo Response消息用于维持控制通道通信。

7-1　回显请求

对CAPWAP控制消息来说，Echo Request消息是一种保持激活机制。

Echo Request由身处Image Data或Run状态的WTP定期发送(参阅第2-3节)，以便确定WTP和AC间的控制连接状态。当EchoInterval计时器到期，WTP发送Echo Request消息。

在Run状态期间，WTP发送Echo Request消息。AC不发送这条消息。

在Echo Request消息中**可以**包括下述消息要素：

- Vendor Specific Payload，参阅第4-6-39节

AC收到Echo Request消息后，用Echo Response消息响应。

7-2　回显响应

Echo Response 消息确认 Echo Request 消息。

Echo Response 消息由 AC 在收到 Echo Request 消息后发送。发送 Echo Response 消息后，AC **应当**复位它的 EchoInterval 计时器(参阅第 4-7-7 节)。如果该计时器到期，AC 没有收到另一个 Echo Request 消息或其他控制消息，AC **应当**认为该 WTP 不再可达。

Echo Response 消息由 AC 在 Run 状态期间发送。WTP 不发送这条消息。

在 Echo Response 消息中**可以**包括下述消息要素：

- Vendor Specific Payload，参阅第 4-6-39 节

当 WTP 收到 Echo Response 消息时，它将 EchoInterval 初始化到配置的值。

第 8 章　WTP 配置管理

WTP Configuration 消息用于在 AC 和 WTP 间交换配置信息。

8-1　配置一致性

CAPWAP 协议在 WTP 配置管理上较为灵活。WTP 可以采用两种方式之一运行，具体由实现决定：

1、WTP 不保留配置，接受 AC 提供的配置。

2、WTP 在本地非易失性存储器中保存 AC 提供的配置参数(不是默认值)，在 WTP 开机初始化阶段强制执行。

如果 WTP 选择本地保存配置，CAPWAP 协议状态机定义 Configure 状态，它允许配置交换。在 Configure 状态，通过 Configuration Status Request 消息，WTP 发送它目前的基本配置给 AC。基本配置不是默认参数。例如，在 CAPWAP 协议中，默认天线配置是内部全向天线。没有内部天线或已经由 AC 明确配置成使用外部天线的 WTP，在配置阶段发送它的天线配置，让 AC 注意到 WTP 目前的配置。

一旦 WTP 提供它的配置给 AC，AC 发送它的配置给 WTP。这使 WTP 能够接收来自 AC 的配置和策略。

AC 保留每个激活 WTP 配置副本。不需要版本管理或其他识别配置改变的方法。如果 WTP 不再处于激活状态，AC **可以**删除失活 WTP 的配置。如果 WTP 失效，或连接到新 AC，WTP 提供它的基本配置参数，让新的 AC 能够了解其配置。

这种模式确保即使 AC 出现故障也不会停止 WTP 服务，而是改由另一个 AC 向该 WTP 提供服务。新 AC 使用 WTP 配置变动自动更新，省去了 AC 间原本需要的通信，不需要所有 ACs 了解网络中所有 WTPs 的配置。

一旦CAPWAP协议进入Run状态，WTPs开始提供服务。通常，虽然网络可用，但管理员需要改变配置。因此，Configuration Update Request由AC发送给WTP，以便在运行时修改配置。

8-1-1　配置灵活性

CAPWAP协议很灵活，也可以通过改变设计和功能特性来配置和管理WTPs。当WTP首次发现AC时，它提供主要的功能信息，这些信息与交换的它的MAC类型和帧性质有关。AC适当配置WTP。AC也建立该WTP的相应内部状态。

8-2　配置状态请求

Configuration Status Request 消息由 WTP 发送给 AC，用于传递它目前的配置。

Configuration Status Request 消息携带特别绑定的消息要素。指定义这种结构的适当绑定。

如果 AC 收到 Configuration Status Request 消息，它根据消息内容行动，用 Configuration Status Response 消息响应 WTP。

Configuration Status Request 消息包括多个 Radio Administrative State 消息要素，一个用于 WTP，一个用于 WTP 中的每个无线电设备。

Configuration Status Request 消息由 WTP 在 Configure 状态期间发送。AC 不发送这条消息。

在 Configuration Status Request 消息中**必须**包括下述消息要素。

- AC Name，参阅第 4-6-4 节
- Radio Administrative State，参阅第 4-6-33 节
- Statistics Timer，参阅第 4-6-38 节
- WTP Reboot Statistics，参阅第 4-6-47 节

在 Configuration Status Request 消息中**可以**包括下述消息要素。

- AC Name with Priority，参阅第 4-6-5 节
- CAPWAP Transport Protocol，参阅第 4-6-14 节
- WTP Static IP Address Information，参阅第 4-6-48 节
- Vendor Specific Payload，参阅第 4-6-39 节

8-3　配置状态响应

Configuration Status Response 消息由 AC 发送，为 AC 提供一种机制，来取代 WTP 请求的配置。

Configuration Status Response 消息由 AC 在收到 Configuration Status Request 消息后发送。

Configuration Status Response 消息携带特别绑定的消息要素。指定义这种结构的适当绑定。

如果 WTP 收到 Configuration Status Response 消息，它根据消息内容适当行动。如果 Configuration Status Response 消息包括 Radio Operational State 消息要素，该消息要素引起其中一个无线电设备的运行状态发生变化，WTP 发送 Change State Event 给 AC，作为对状态改变的确认。

Configuration Status Response 消息由 AC 在 Configure 状态期间发送。WTP 不发送这条消息。

在 Configuration Status Response 消息中**必须**包括下述消息要素。

- CAPWAP Timers，参阅第 4-6-13 节
- Decryption Error Report Period，参阅第 4-6-18 节
- Idle Timeout，参阅第 4-6-24 节
- WTP Fallback，参阅第 4-6-42 节

在 Configuration Status Response 消息中**必须**包括下述一个或两个消息要素：

- AC IPv4 List，参阅第 4-6-2 节
- AC IPv6 List，参阅第 4-6-3 节

在 Configuration Status Response 消息中**可以**包括下述消息要素。

- WTP Static IP Address Information，参阅第 4-6-48 节
- Vendor Specific Payload，参阅第 4-6-39 节

8-4　配置更新请求

Configuration Update Request 消息由 AC 在 Run 状态发送给 WTP，用于修改 WTP 的配

置，尽管 WTP 在运行中。

如果 WTP 收到 Configuration Update Request 消息，它用 Configuration Update Response 消息响应，该消息带有指出配置请求结果的 Result Code 消息要素。

同时在 Run 状态期间，AC 包括强制 WTP 更新它的固件的 Image Identifier 消息要素(参阅第 4-6-27 节)。如果 WTP 确定在 Image Identifier 消息要素中指定的版本不在它的非易失性存储器中，通过发送包括 Initiate Download 消息要素(参阅第 4-6-29 节)的 Image Data Request(参阅第 9-1-1 节)，WTP **可以**着手下载要求的固件。

Configuration Update Request 由 AC 在 Run 状态期间发送。WTP 不发送这条消息。

在 Configuration Update 消息中**可以**包括下述一个或多个消息要素：

- AC Name with Priority，参阅第 4-6-5 节
- AC Timestamp，参阅第 4-6-6 节
- Add MAC ACL Entry，参阅第 4-6-7 节
- CAPWAP Timers，参阅第 4-6-13 节
- Decryption Error Report Period，参阅第 4-6-18 节
- Delete MAC ACL Entry，参阅第 4-6-19 节
- Idle Timeout，参阅第 4-6-24 节
- Location Data，参阅第 4-6-30 节
- Radio Administrative State，参阅第 4-6-33 节
- Statistics Timer，参阅第 4-6-38 节
- WTP Fallback，参阅第 4-6-42 节
- WTP Name，参阅第 4-6-45 节
- WTP Static IP Address Information，参阅第 4-6-48 节
- Image Identifier，参阅第 4-6-27 节
- Vendor Specific Payload，参阅第 4-6-39 节

8-5　配置更新响应

Configuration Update Response 消息是 Configuration Update Request 消息的确认消息。

Configuration Update Response 消息由 WTP 在收到 Configuration Update Request 消息后发送。

当 AC 收到 Configuration Update Response 消息时，结果代码指出 WTP 是否成功接受该配置。

Configuration Update Response 消息由 WTP 在 Run 状态期间发送。AC 不发送这条消息。

在 Configuration Update 消息中**必须**包括下述消息要素。

- Result Code，参阅第 4-6-35 节

在 Configuration Update Response 消息中**可以**包括下述消息要素。

- Radio Operational State，参阅第 4-6-34 节
- Vendor Specific Payload，参阅第 4-6-39 节

8-6　改变状态事件请求

Change State Event Request 消息由 WTP 用于两个主要目的：

- WTP 在收到来自 AC 的 Configuration Status Response 消息后紧接着发送，WTP 使用 Change State Event Request 消息提供对 WTP 无线电设备的运行状态更新，以及证实由 AC 提供的配置成功得到应用。
- 在 Run 状态期间发送，WTP 使用 Change State Event Request 消息通知 AC，在 WTP 的无

线电设备运行状态中出现意外改变。

当 AC 收到 Change State Event Request 消息时，它用 Change State Event Response 消息响应，并根据需要修改它的该 WTP 数据结构。如果 AC 收到错误，根据本地策略，AC **可以**决定不向该 WTP 提供服务，并转换到 Reset 状态。

Change State Event Request消息由WTP发送，用于针对在Configuration Status Response消息中要求的配置，向AC确认或报告错误状况。Change State Event Request消息包括Result Code消息要素，它指出配置是否成功应用。如果WTP不能应用指定的配置要求，WTP通过包括一个或多个Returned Message Element消息要素(参阅第4-6-36节)指出失败。

Change State Event Request 消息由 WTP 在 Configure 或 Run 状态发送。AC 不发送这条消息。WTP **可以**在传送该响应前将它的配置保存在永久存储器。然而，这由具体实现决定，这里没有要求。

在 Change State Event Request 消息中**必须**包括下述消息要素。

- Radio Operational State，参阅第 4-6-34 节
- Result Code，参阅第 4-6-35 节

在 Change State Event Request 消息中**可以**包括下述一个或多个消息要素：

- Returned Message Element(s)，参阅第 4-6-36 节
- Vendor Specific Payload，参阅第 4-6-39 节

8-7　改变状态事件响应

Change State Event Response 消息确认 Change State Event Request 消息。

Change State Event Response 消息由 AC 发送，用于响应 Change State Event Request 消息。

Change State Event Response 消息由 AC 在 Configure 或 Run 状态期间发送。WTP 不发送这条消息。

在 Change State Event Response 消息中**可以**包括下述消息要素：

- Vendor Specific Payload，参阅第 4-6-39 节

收到 Change State Event Response 消息，WTP 不采取任何行动。

8-8　清除配置请求

Clear Configuration Request 消息用于复位 WTP 配置。

Clear Configuration Request 消息由 AC 发送，用于要求 WTP 将它的配置复位到厂家默认配置。在 Run 状态期间发送 Clear Configuration Request 消息。

Clear Configuration Request 由 AC 在 Run 状态期间发送。WTP 不发送这条消息。

在 Clear Configuration Request 消息中**可以**包括下述消息要素：

- Vendor Specific Payload，参阅第 4-6-39 节

当 WTP 收到 Clear Configuration Request 消息时，它将它的配置复位到厂家默认配置。

8-9　清除配置响应

Clear Configuration Response 消息由 WTP 在收到 Clear Configuration Request 消息并将它的配置参数复位到厂家默认值后发送。

Clear Configuration Response 消息由 WTP 在 Run 状态期间发送。AC 不发送这条消息。

在 Clear Configuration Response 消息中**必须**包括下述消息要素：

- Result Code，参阅第 4-6-35 节

在 Clear Configuration Response 消息中**可以**包括下述消息要素：

- Vendor Specific Payload，参阅第 4-6-39 节

第 9 章　设备管理操作

本章定义负责调试、收集统计数据、日志记录和固件管理的 CAPWAP 操作。在本章中定义的管理操作由 AC 使用，或者是推送信息给 WTP/从 WTP 抽取信息，或者要求 WTP 重新启动。本章不讨论 AC 自身的管理，并且假设 AC 已配置好，可以使用。

9-1　固件管理

这一节介绍使用 CAPWAP 协议下载固件流程。固件可以在 Image Data 或 Run 状态期间下载间。前者允许在启动时下载，而后者用于存在激活的 CAPWAP 会话时触发下载。重要的是要注意到 CAPWAP 协议没有为 AC 提供能力，使其能够识别 WTP 提供的固件消息是否正确，或者 WTP 是否适当保存固件(更多信息参阅第 12-10 节)。

图 6 演示在 Image Data 状态，WTP 执行固件更新的例子。在此例中，WTP 还没有要求的固件(Image Identifier = x)，并从 AC 下载映像。

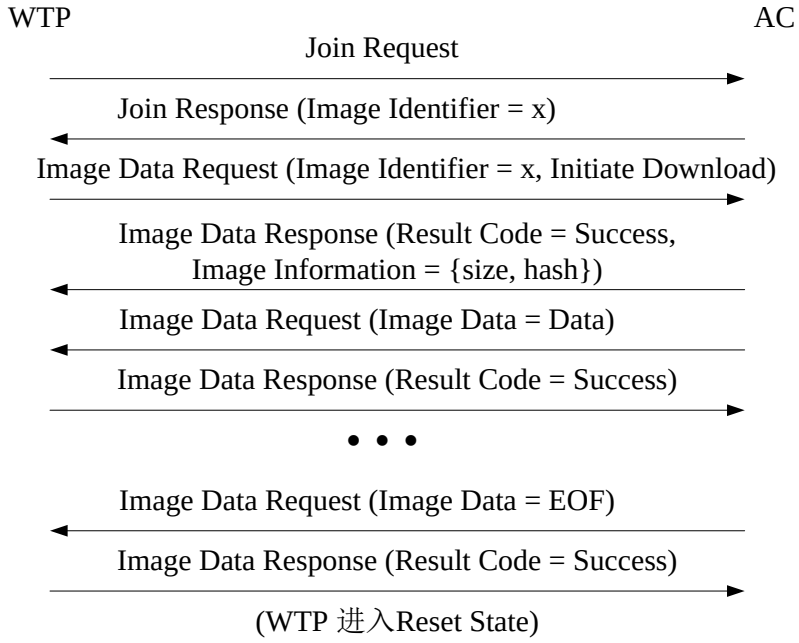


图 6　WTP 固件下载例 1

在图 7 的例子中，WTP 的非易失性存储器中有 AC 指定的映像，但不是 WTP 目前运行的映像。在这种情况，WTP 选择不下载固件，并且立即复位到要求的映像。

图 7　WTP 固件下载例 2

在图 8 的例子中，WTP 在 Run 状态期间执行固件更新。这个固件更新模式允许 WTP 下载它的映像，同时继续提供服务。WTP 不会自动复位，直到 AC 用 Reset Request 消息通知它。

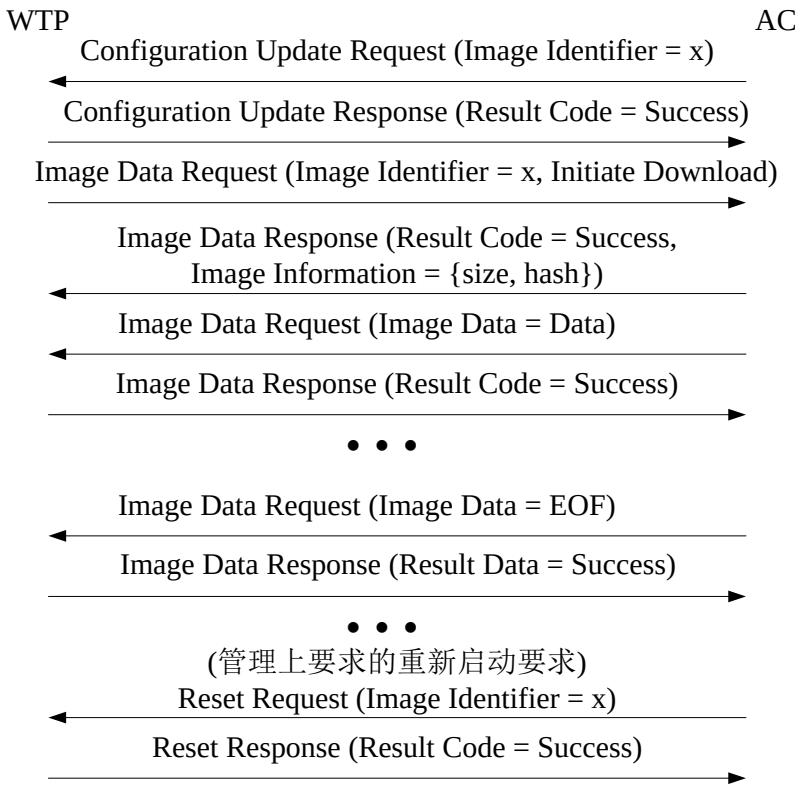


图 8　WTP 固件下载例 3

图 9 提供另一个在 Run 状态期间固件下载例子。在这个例子中，WTP 的非易失性存储器中有 AC 指定的映像。WTP 选择不下载固件。一旦收到来自 AC 的 Reset Request 消息，WTP 复位。

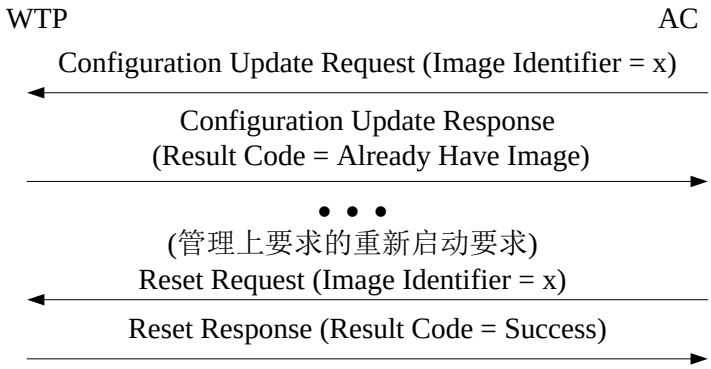


图 9　WTP 固件下载例 4

9-1-1　映像数据请求

Image Data Request 消息用于更新 WTP 上的固件。这个消息和它的伙伴 Response 消息由 AC 用于确保在每个 WTP 上正在运行的映像是适当的。

Image Data Request 消息在 WTP 和 AC 间交换，以便下载新的固件映像给 WTP。当 WTP 或 AC 收到 Image Data Request 消息时，接收者用 Image Data Response 消息响应。规定由 Image Data Request 消息中包含的消息要素决定该要求的意图。

做出新固件要下载到 WTP 的决策有两种方式：

当 WTP 加入 AC 时，Join Response 消息包括 Image Identifier 消息要素，该消息要素通知预期固件将要运行其上的 WTP。如果 WTP 目前没有要求的固件版本，WTP 发送 Image Data Request 消息，该消息带有适当的 Image Identifier 消息要素。如果 WTP 在它的非易失性闪存中已经有要求的固件，但是不是它目前运行的映像，WTP 简单复位，以便运行适当的固件。

当 WTP 处在 Run 状态期间，AC 通过发送带 Image Identifier 消息要素的 Configuration Update Request 消息，有可能引起 WTP 启动固件下载。这将引起 WTP 发送带 Image Identifier 和 Initiate Download 消息要素的 Image Data Request。注意，如果用这种方法下载固件，WTP 在下载完成后不会自动复位。仅当收到来自 AC 的 Reset Request 消息时，WTP 才会复位。如果在 WTP 自己的非易失性存储器中已经有要求的固件版本，WTP 不会发送 Image Data Request 消息，不会用带设置为 Image Already Present 的 Result Code 的 Configuration Update Response 消息进行响应。

无论下载是如何启动的，一旦 AC 收到带 Image Identifier 消息要素的 Image Data Request 消息，AC 通过发送包括 Image Data 消息要素的 Image Data Request 消息，开始传送流程。传送流程一直持续到固件映像传送完成。

Image Data Request 消息由 WTP 或 AC，在 Image Data 或 Run 状态期间发送。

在 Image Data Request 消息中**可以**包括下述消息要素：

- CAPWAP Transport Protocol，参阅第 4-6-14 节
- Image Data，参阅第 4-6-26 节
- Vendor Specific Payload，参阅第 4-6-39 节

如果是由 WTP 发送，在 Image Data Request 消息中**可以**包括下述消息要素：

- Image Identifier，参阅第 4-6-27 节
- Initiate Download，参阅第 4-6-29 节

9-1-2 映像数据响应

Image Data Response 消息确认 Image Data Request 消息。

发送 Image Data Response 消息，用于响应收到的 Image Data Request 消息，从而确认收到 Image Data Request 消息。包括 Result Code 是为了指出先前发送的 Image Data Request 消息是否无效。

Image Data Response 消息由 WTP 或 AC 在 Image Data 或 Run 状态期间发送。

在 Image Data Response 消息中**必须**包括下述消息要素：

- Result Code，参阅第 4-6-35 节

在 Image Data Response 消息中**可以**包括下述消息要素：

- Vendor Specific Payload，参阅第 4-6-39 节

如果由 AC 发送，在 Image Data Response 消息中**可以**包括下述消息要素：

- Image Information，参阅第 4-6-28 节

一旦收到指出错误的 Image Data Response 消息，WTP **可以**重发先前的 Image Data Request 消息，或通过转换到 Reset 状态，放弃对该 WTP 的固件下载。

9-2 复位请求

Reset Request 消息用于引起 WTP 重新启动。

Reset Request 消息由 AC 发送，以便引起 WTP 重新启动它的运行。如果 AC 包括 Image Identifier 消息要素(参阅第 4-6-27 节)，该消息要素指示 WTP 一旦重新启动**应当**使用那个软件版本。

Reset Request 由 AC 在 Run 状态期间发送。WTP 不发送这条消息。

在 Reset Request 消息中**必须**包括下述消息要素：

- Image Identifier，参阅第 4-6-27 节

在 Reset Request 消息中**可以**包括下述消息要素：

- Vendor Specific Payload，参阅第 4-6-39 节

当 WTP 收到 Reset Request 消息时，它用指示成功的 Reset Response 消息响应，接着重新启动自己。如果 WTP 不能写到它的非易失性存储器，为了确保它运行在 Image Identifier 消息要素指出的、所要求软件版本，它**可以**发送适当的 Result Code 消息要素，但是**必须**重新启动。如果 WTP 不能复位，包括硬件复位，WTP 发送带 Result Code 消息要素(指出失败)的 Reset Response 消息给 AC。AC 不再向该 WTP 提供服务。

9-3 复位响应

Reset Response 消息确认 Reset Request 消息。

Reset Response 消息由 WTP 在收到 Reset Request 消息后发送。

Reset Response 由 WTP 在 Run 状态期间发送。AC 不发送这条消息。

在 Reset Response 消息中可以**包括**下述消息要素。

- Result Code，参阅第 4-6-35 节
- Vendor Specific Payload，参阅第 4-6-39 节

如果 AC 收到成功的 Reset Response 消息，AC 通知 WTP 重新启动它的运行。收到指出失败的 Reset Response 消息的 AC 可以选择不再向该 WTP 提供服务。

9-4 WTP 事件请求

WTP Event Request 消息由 WTP 用于向它的 AC 发送信息。WTP Event Request 消息**可以**定期发送，也可以作为 WTP 上偶发事件的响应发送。例如，WTP **可以**收集统计数据并使用 WTP Event Request 消息发送这些统计数据给 AC。

当 AC 收到 WTP Event Request 消息时，它用 WTP Event Response 消息响应。

WTP 通过包含 Delete Station 消息要素，通知 AC，它不再为该站点提供服务。这可能是 Idle Timeout(参阅第 4-6-24 节)结果，由于资源短缺，或其他原因。

WTP Event Request 消息由 WTP 在 Run 状态期间发送。AC 不发送这条消息。

WTP Event Request 消息**必须**包括下列一个或多个消息要素，或为特定无线技术定义的消息要素。在 WTP Event Request 消息中**可以**包括不止一个列出的消息要素。

- Decryption Error Report，参阅第 4-6-17 节
- Duplicate IPv4 Address，参阅第 4-6-22 节
- Duplicate IPv6 Address，参阅第 4-6-23 节
- WTP Radio Statistics，参阅第 4-6-46 节
- WTP Reboot Statistics，参阅第 4-6-47 节
- Delete Station，参阅第 4-6-20 节
- Vendor Specific Payload，参阅第 4-6-39 节

9-5 WTP 事件响应

WTP Event Response 消息确认收到 WTP Event Request 消息。

WTP Event Response 消息由 AC 在收到 WTP Event Request 消息后发送。

WTP Event Response 消息由 AC 在 Run 状态期间发送。WTP 不发送这条消息。

在 WTP Event Response 消息中**可以**包括下述消息要素：

• Vendor Specific Payload，参阅第 4-6-39 节

9-6　数据传送

这一节介绍 CAPWAP 协议使用的数据传送流程。数据传送机制用于上传 WTP 中可获得的信息给 AC，诸如故障和调试信息。数据传送消息仅可以在 Run 状态期间交换。

图 10 为 AC 要求 WTP 提供它的最新故障文件的例子。通过 Data Transfer Response，一旦 WTP 确认它有信息发送，它发送它自己的 Data Transfer Request。 一旦收到，AC 用 Data Transfer Response 响应，这个交换一直持续，直到 WTP 发送 Data Transfer Data 消息要素，该消息要素指出 End of File (EOF)。

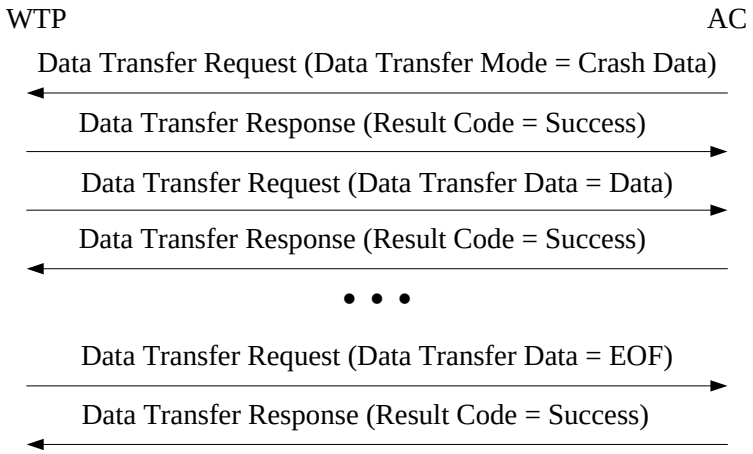


图 10　WTP 数据传送例 1

图 11 为 AC 要求 WTP 发送它的最新故障文件例子。然而，在这个例子中，WTP 没有任何故障信息需要发送，因此，WTP 发送带有指出错误用的 Result Code 的 Data Transfer Response 消息。

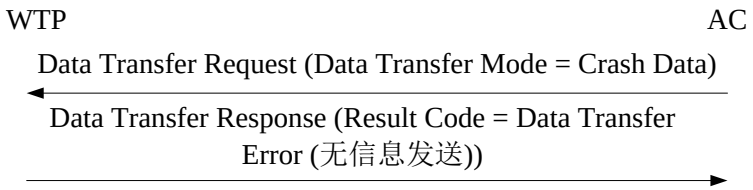


图 11　WTP 数据传送例 2

9-6-1　数据传送请求

Data Transfer Request 消息用于将来自 WTP 的调试信息传递给 AC。

Data Transfer Request 消息可以由 AC 或 WTP 发送。当 AC 使用时，它用于要求把数据从 WTP 传送给 AC， 并且包括 Data Transfer Mode 消息要素，该消息要素规定 AC 想要的信息。Data Transfer Request 由 WTP 发送，以便通过 Data Transfer Data 消息要素传递实际数据给 AC。

鉴于 CAPWAP 协议尽量减少对 WTPs 直接管理的理念，Data Transfer Request 是重要的故障诊断工具，它由 AC 用于检索能够在 WTP 上获得的信息。例如，某些 WTP 实现可以保存故障信息以方便管理者鉴别软件故障。Data Transfer Request 消息可用于从 WTP 发送这样的信息给 AC。另一种可能的应用是允许 WTP 中的远程调试器功能使用 Data Transfer Request 消息，发送控制台输出给 AC，用于调试。

当 WTP 或 AC 收到 Data Transfer Request 消息，用 Data Transfer Response 消息响应 AC 或 WTP。AC **可以**记录经 Data Transfer Data 消息要素收到的信息。

Data Transfer Request 消息由 WTP 或 AC 在 Run 状态期间发送。

由 AC 发送时，Data Transfer Request 消息**必须**包括下述消息要素：

- Data Transfer Mode，参阅第 4-6-16 节

由 WTP 发送时，Data Transfer Request 消息**必须**包括下述消息要素：

- Data Transfer Data，参阅第 4-6-15 节

无论是由 AC 还是由 WTP 发送 Data Transfer Request，在 Data Transfer Request 消息中**可以**包括下述消息要素：

- Vendor Specific Payload，参阅第 4-6-39 节

9-6-2 数据传送响应

Data Transfer Response 消息确认 Data Transfer Request 消息。

发送 Data Transfer Response 消息，以便响应收到的 Data Transfer Request 消息。当由 WTP 发送时，Result Code 消息要素用于指出由 AC 要求的数据传送是否能够完成。当由 AC 发送时，Result Code 消息要素用于指出收到在 Data Transfer Request 消息中发送的数据。

Data Transfer Response 消息由 WTP 或 AC 在 Run 状态期间发送。

Data Transfer Response 消息中**必须**包括下述消息要素：

- Result Code，参阅第 4-6-35 节

在 Data Transfer Response 消息中**可以**包括下述消息要素：

- Vendor Specific Payload，参阅第 4-6-39 节

一旦收到 Data Transfer Response 消息，WTP 发送更多信息，如果有更多可用信息。

第 10 章 站点会话管理

这一章中的消息由 AC 使用，用于创建、修改或删除 WTPs 上的站点会话状态。

10-1 站点配置请求

Station Configuration Request 消息用于创建、修改或删除 WTP 上的站点会话状态。该消息由 AC 发送给 WTP，**可以**包括一个或多个消息要素。这个 CAPWAP Control 消息的消息要素包括的信息通常是高度技术特定信息。在这个控制消息中包括的消息要素的定义请参考适当的关联文档。

Station Configuration Request 消息由 AC 在 Run 状态期间发送。WTP 不发送这条消息。

在 Station Configuration Request 消息中**可以**包括下述 CAPWAP Control 消息要素。在 Station Configuration Request 消息中**可以**包括列出的不止一个消息要素：

- Add Station，参阅第 4-6-8 节
- Delete Station，参阅第 4-6-20 节
- Vendor Specific Payload，参阅第 4-6-39 节

10-2 站点配置响应

Station Configuration Response 消息用于确认先前收到的 Station Configuration Request 消息。

Station Configuration Response 消息由 WTP 在 Run 状态期间发送。AC 不发送这条消息。

在 Station Configuration Response 消息中**必须**包括下述消息要素：

- Result Code，参阅第 4-6-35 节

在 Station Configuration Response 消息中**可以**包括下述消息要素：

- Vendor Specific Payload，参阅第 4-6-39 节

Result Code 消息要素指出要求的配置已成功应用，或者在 WTP 上发生与 Station Configuration Request 消息处理有关的错误。

第 11 章　NAT 考虑

在 3 种特定情况下，NAT 部署可以与启动 CAPWAP 的部署一起使用。第一种情况是一种配置，单台 WTP 放在 NAT 系统后面。因为所有通信由 WTP 发起，并且所有通信是在 IP 上，使用两个 UDP 端口执行，在这种配置中 CAPWAP 协议容易穿越 NAT 系统。

第二种情况，两个或多个WTPs部署在同一NAT系统后面。这里，AC将收到来自相同IP地址的多个连接请求，因此，不能单独使用WTP的IP地址绑定CAPWAP Control和Data通道。CAPWAP Data Check状态，它建立数据平面连接和通知CAPWAP Data Channel Keep-Alive，包括Session Identifier消息要素，该消息要素用于绑定控制和数据平面。使用Session Identifier消息要素，能够让AC匹配来自同一NAT系统后面多个WTPs的控制流和数据流(多个WTPs共享相同IP地址)。CAPWAP实现也**必须**使用在任何加密CAPWAP通道上的DTLS会话信息，以便使控制和数据平面的源合法化，正如第12-2节所述。

第三种配置中，AC 被部署在 NAT 后面。这时， WTP 不能到达 AC，除非在 NAT 上做特殊规则配置，以便转换地址并重新定向 CAPWAP 消息到 AC。这种部署存在两个问题。首先，AC 使用 CAPWAP Control IPv4 Address 消息要素和 CAPWAP Control IPv6 Address 消息要素通告它的接口和相应的 WTP 负载。这个消息要素是强制性的，但是包含仅在由 AC 使用的私有地址空间才是合法的 IP 地址，WTP 不能到达该 IP 地址。如果 WTP 检测到 NAT，WTP **必须不**使用这些消息要素中的信息(正如在第 4-6-14 节的 CAPWAP Transport Protocol 消息要素中介绍的)。其次，因为 WTP 不能使用这些地址，这样一来实际上禁用了 CAPWAP 协议的负载均衡能力(参阅第 6-1 节)。此外，AC 或许有配置的 NAT 的地址，AC 可能将该 NAT 的地址放在两个控制地址消息要素中的任何一个中，NAT 需要做相应配置。为使 CAPWAP WTP 或 AC 检测到中间体是否存在，Join Request(参阅第 6-1 节)和 Join Response(参阅第 6-2 节)都包括 CAPWAP Local IPv4 Address (参阅第 4-6-11 节)或 CAPWAP Local IPv6 Address(参阅第 4-6-12 节)消息要素。一旦收到这两个消息之一，如果分组的源 IP 地址不同于这些消息要素中任何一个消息要素内包含的地址，表示存在中间体。

为使 CAPWAP 兼容网络中可能的中间体，各 CAPWAP 实现**必须**通过相同端口(在该端口上，实现接收来自给定对端的流量)发送返回流量。此外，任何由 CAPWAP 节点产生的、主动提供的请求**必须**在相同端口发送。

注意，这个中间体检测技术并不十分安全。如果分配给 NAT 的公共 IP 地址等于 AC 使用的私有 IP 地址，WTP 的检测可能失败。这个失败会引起各种协议错误，所以，在部署上必须确保 NAT 的 IP 地址与 ACs 的 IP 地址不同。

CAPWAP 协议可以通过 AC List 消息要素，通告支持一组 WTPs 的所有 AC 身份。当 WTP 检测到 AC 位于中间体后面时，WTP **必须**忽略这个功能。

CAPWAP 协议允许 AC 使用 WTP Static IP Address Information 消息要素，在 WTP 上配置静态 IP 地址。在 NAT 环境，**不应当**使用这个消息要素，除非管理者熟悉该 WTP 私有网络内部 IP 地址方案，不依靠被 AC 看见的公共地址。

当 WTP 检测到重复地址情况，它生成给 AC 的消息，该消息包括 Duplicate IP Address 消息要素。嵌入在这个消息要素内的 IP 地址不同于被 AC 看见的公共 IP 地址。

第 12 章　安全考虑

这一章介绍 CAPWAP 协议安全考虑。其中也涉及与 CAPWAP 一起使用的协议的安全考虑。

12-1 CAPWAP 安全

正如目前规定的，CAPWAP协议位于由无线链路层协议(例如，IEEE 802.11i)规定的安全机制与认证、授权和计费(Authentication、Authorization和Accounting, AAA)之间。CAPWAP的一个目标是使用一系列预先确定的信任关系，逐步建立STA和WTP间的信任，参阅图12。

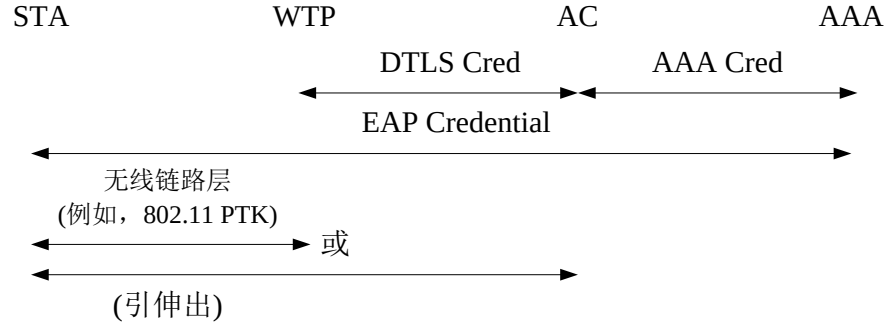


图 12 STA 会话建立

在 CAPWAP 内，DTLS 用于保护 WTP 和 AC 间的链路。除了保护控制消息以外，它也是这条建立链路层密钥信任链中的链路。因此，更多倚重 DTLS。

在一些 CAPWAP 部署场景，WTP 和 AC 间有两条通道：承载 CAPWAP Control 消息的控制通道，和数据通道，在其上 AC 和 WTP 间的客户端数据分组被隧道化。典型情况，控制通道由 DTLS 保护，而数据通道没有保护。

平行使用受保护通道和不受保护通道值得特别关注，但不会产生威胁。有两个可能的担忧：企图将受保护数据转换成不受保护数据，和企图将不受保护数据转换成受保护数据。下面讨论如何处理这两个担忧。

12-1-1 转换受保护数据为不受保护数据

因为 CAPWAP 不支持仅认证的密码(即，所有支持的密码套件包括加密和认证)，将受保护数据转换成不受保护数据不可能实现。因为加密数据(在理想情况下)难以和随机数据区别，加密分组被当作标准格式分组的概率实际上为 0。

12-1-2 转换不受保护数据为受保护数据(插入)

由于使用消息认证，攻击者不可能伪造受保护记录。于是，不可能将不受保护记录转换成受保护记录。

12-1-3 删除受保护记录

虽然预期底层 CAPWAP 协议具有内在安全性，然而不是无法检测到，攻击者能够从数据流中删除受保护的记录。在最糟糕情况，攻击者能够重复删除相同记录，导致 CAPWAP 会话超时和重启。这是高效 DoS 攻击，可由中间人完成，无论选择何种 CAPWAP 协议安全机制。

12-1-4 插入不受保护记录

攻击者能够把分组加到不受保护的通道中，但是如果因此导致序列号不同步很容易引起注意。只有在攻击者是中间人(Man In The Middle, MITM)的情况能够插入分组而又不被察觉。

这是通道缺乏保护的结果，不是根源于 CAPWAP 安全机制的新威胁。

12-1-5 应用 MD5

Image Information 消息要素(参阅第 4-6-28 节)使用 MD5 计算哈希(hash)字段。映像文件的认证和完整性由 DTLS 保护，在这一背景下，MD5 不用作加密的安全哈希值，仅作为基本校验和。因此，不认为使用 MD5 是安全漏洞，不提供算法灵活的机制。

12-1-6 CAPWAP 分段

RFC 4963 [RFC4963]描述了可能的安全漏洞，即，恶意的实体可能通过注入分段“掺杂”数据流。通过发送“高”分段(带有偏移量大于 0 的分段)，而且这些分段带有伪造的源地址，攻击者能够蓄意引起掺杂。在 CAPWAP Data 通道上使用 DTLS 可以避免这种可能的漏洞。

12-2 会话 ID 安全

因为 DTLS 不输出唯一的会话标识符，在 DTLS 层和 CAPWAP 层之间没有精确的协议绑定。因此，实现**必须**提供执行这种绑定的机制。例如，AC **必须不能**将解密的 DTLS 控制分组，关联到只根据分组首部中 Session ID 而确定的具体 WTP 会话。相反，应当根据哪一个 DTLS 会话解密了该分组进行鉴别。否则，通过修改加密 CAPWAP Header 中的 Session ID，一个认证的 WTP 可能欺骗另一个认证的 WTP。

应当注意到，如果不加密 CAPWAP Data 通道，WTP Session ID 暴露，可能被对手和其他 WTPs 获知。这将允许伪造数据通道流量的源。然而，对于不加密的数据通道这不是什么意外事。如果加密数据通道，Session ID 不会暴露，因此，可将其安全用于关联数据和控制通道。128 位长的 Session ID 降低了在线猜测攻击(那里，敌对的、经过认证的 WTP 尝试将它自己的数据通道与另一个 WTP 的控制通道联系起来)的风险。注意，对于加密的数据通道，Session ID 应当仅用于与紧跟在发起 DTLS 握手后的第一个分组关联。之后的相关应当通过识别分组 DTLS 会话代替。

12-3 发现或 DTLS 设置攻击

因为 Discovery Request 消息采用明文发送，尤其重要的是 AC 实现**不**假设从 WTP 接收 Discovery Request 消息，这暗示 WTP 已经重新启动，因此拆除任何激活的 DTLSW 会话。Discovery Request 消息很容易被恶意设备欺骗，所以在收到 DTLSSessionEstablished 通知，指出 WTP 获得认证以前，AC 维持两套独立的 WTP 状态很重要。一旦新的 DTLS 会话成功建立，可以删除任何涉及旧会话的状态。

类似，如果 AC 正在进入 DTLS Setup 阶段，它**不应当**假设 WTP 已经复位，因此，在该 DTLS 会话成功建立起来以前不应当抛弃激活的状态。虽然在 AC 上 HelloVerifyRequest 提供一些应对 DoS 攻击的保护，有能力在合法地址上接收分组的敌对方(或者出现故障或错误配置的 WTP)可以反复尝试与 AC 实现 DTLS 握手，潜在造成资源短缺状况。如果 FailedDTLSSessionCount 或 FailedDTLSAuthFailCount 计数器到达 MaxFailedDTLSSessionRetry 变量值(参阅第 4-8 节)，实现**可以**在一段时间内选择速率受限的新 DTLS 握手。**推荐**：选择执行限制速率的实现使用随机抛弃技术，而不是模仿该 WTP 的不理智行为。这将确保来自合法 WTPs 的消息以一定的概率得到响应，即使在面临严重 DoS 攻击情况下。

某些 CAPWAP 实现可能希望限制 DTLS 设置流程为仅包括已经在访问控制列表中配置的对端，仅授权那些客户端发起 DTLS 握手。注意，这对减轻对 DTLS 层的拒绝服务攻击的作用很小，因为 DTLS 已经使用客户端一侧的 cookies 来尽量减小处理器消耗攻击。

12-4 伴随 DTLS 会话的干扰

如果 WTP 或 AC 反复收到造成 DTLS 认证或解密失败的分组，这可能指出 AC 和 WTP 间 DTLS 不同步，链路不容易检测到的位误码，或存在试图破坏 DTLS 会话的攻击。

在状态机(参阅第 2-3 节)中，频繁收到带认证或解密错误的 DTLS 分组会触发转换到 DTLS Tear Down (TD)状态。应慎重选择决定何时移动到拆除状态的门限或技术。能够轻易转换到DTLS TD可以方便地检测到故障设备，但会带来拒绝服务攻击。增加转换到DTLS TD的难度能够较好防范拒绝服务攻击，但会使检测和复位出故障会话更加困难。实施者应当慎重设置这个策略。

12-5 CAPWAP 预配置

为使 CAPWAP 能够建立与对端的安全通信，有必要预先配置 WTP 和 AC 上的某些层次。这一节将详述最低限度的配置参数数量。

当使用预共享密钥时，必须为每个可能与其建立 DTLS 会话的对端配置预共享密钥。为支持这种运行模式，可以在 AC 或 WTP 上配置下表中的一个或多个条目：

- 身份(Identity)：对端 AC 或 WTP 身份。这个格式**可以**采用 IP 地址或主机名称的形式(后者需要使用 DNS 解析到 IP 地址)。
- 密钥(Key)：当建立 DTLS 会话时与对端一起使用的预共享密钥(更多介绍参阅第 12-6 节)。
- PSK 身份(Identity)：与预配置密钥关联的身份提示(更多介绍参阅第 2-4-4-4 节)。

如果使用证书，需要预先配置下述项目：

- 设备证书(Device Certificate)：本地设备证书(更多介绍参阅第 12-7 节)。
- 信任锚(Trust Anchor)：受信任的根证书链，用于验证从 CAPWAP 对端收到的任何证书。注意，在规定设备上**可以**配置不止一个根证书。

无论采用何种认证方法，需要预先配置下述项目：

- 访问控制列表(Access Control List)：该表包括一个或多个 CAPWAP 对端身份，以及规则。规则用于决定是否允许与该对端通信(更多介绍参阅第 2-4-4-3 节)。

12-6 在 CAPWAP 中使用预共享密钥

尽管使用预共享密钥可以提供在基于公共密钥部署中没有的部署和配置优势，这种方法也引入大量操作和安全隐患。尤其是，因为密钥一般必须人工输入，通常密钥由人们容易记忆的字或词组构成。这些字或词组被称为“低平均信息量(熵)的密码/密码短语”。

使用低熵预共享密钥，连同密钥通常不经常更新，这些都显著增加了暴露的机会。考虑到这些原因，提出下述建议：

- 如果DTLS使用预共享密钥(Pre-Shared Key, PSK)密码套件，每个WTP**应当**有唯一的PSK。因为WTPs极有可能广泛部署，它们的物理安全没有保证。如果每个WTP的PSK不唯一，密钥重复使用会使一个 WTP 的泄漏导致其他 WTPs 的泄漏。
- **不建议**根据低熵密码生成 PSKs。
- **建议**允许管理员人工配置PSK的实现，也提供随机生成新PSKs的能力，参阅RFC 4086 [RFC4086]。
- 预共享密钥**应当**定期更新。实现**可以**通过提供用于自动密钥生成和定期更新的管理接口完成定期更新，也**可以**通过人工完成。

网络上的每对 WTP 和 AC 组合**应当**有唯一的 PSK。这能阻止多米诺骨牌效应(参阅“AAA 密钥管理指南”[RFC4962])。如果 PSKs 绑定到特定 WTPs，那么有关 PSK 的知识暗示绑定到可以被授权的特定身份。

如果 PSKs 共享，这个设备和身份间的绑定不再可能。一个 WTP 的泄漏会导致另一个 WTP 泄漏，破坏了 CAPWAP 的安全层次结构。因此，**不推荐**使用 WTPs 间共享密钥。

12-7 在 CAPWAP 中使用证书

对于基于公共密钥的 DTLS 部署，每个设备**应当**有唯一的证书，采用授权设备充当 WTP 或 AC 的扩展密钥用法。如果设备没有唯一证书，有理由认为：如果一个设备被泄漏，使用相同证书的任何其他设备也会被泄漏。

证书验证涉及检验大量各类事情。因此，必须验证的内容常常需要依环境而定，许多内容超出本文档范围。在这一节我们提供一些有关证书验证的基本指导。

每台设备负责认证和授权将要与其通信的那些设备。认证必然伴有引导到对对方证书的信任链检验，接着是对端证书本身。实现也**应当**提供验证有关证书还没有被废除的安全方法。注意，如果 WTP 依靠 AC 进行网络连接(例如，AC 是 WTP 直接连接的第二层交换机)，如果泄密的 AC 没有明确允许这样做，WTP 可能不能联系 Online Certificate Status Protocol (OCSP)服务器，或者用其他方法获得最新的 Certificate Revocation List (CRL)。这是难以避免的，除非在 AC 采取有效的物理安全措施和监控措施。

证书验证典型将通过检验来确保证书还没有到期。如果设备有实时时钟，设备**应当**检验证书有效期。如果没有实时时钟，设备**应当**通过其他方法尽最大努力，尝试验证证书有效期。不检验证书的时间有效性，容易使设备受到使用泄密、到期证书发起的中间人攻击，因此，设备应当尽一切努力执行这个验证。

12-8 在 CN 字段中使用 MAC 地址

CAPWAP 协议是已有协议[LWAPP]的演进，它要在大量已经部署的 ACs 和 WTPs 上实现。每台这样的设备在出厂时配有 X.509 证书。这些 X.509 证书在 Common Name (CN)字段使用设备的 MAC 地址。很容易理解在 CN 字段编码 MAC 地址不是最好选择，使用 SubjectAltName 字段更可取。然而，在本标准发布时，没有 URN 规范考虑到在 SubjectAltName 字段使用 MAC 地址。因为这类规范由 IETF 颁布，将来的 CAPWAP 协议版本**可以**要求支持新的 URN 方案。

12-9 AAA 安全

AAA 协议用于分发 Extensible Authentication Protocol (EAP)密钥给 ACs，因此它的安全关乎整个系统安全。如果使用 TLS 或 IPsec，**应当**遵守在 RFC 3539 [RFC3539]中规定的安全原则。

通常，AC 和 AAA 服务器间的链路**应当**使用采用相互认证会话密钥加密的强密码套件确保安全。实现**不应当**仅依赖共享密钥认证的 Basic RADIUS，因为它常常经不起字典攻击，而**应当**使用更强的底层安全机制。

12-10 WTP 固件

CAPWAP 协议定义了 AC 下载新固件给 WTP 的机制。在会话建立期间，WTP 向 AC 提供它的目前固件版本信息。AC 接着决定 WTP 的固件是否需要更新。重要的是应注意到本 CAPWAP 规范明确假设 WTP 正在提供正确固件版本给 AC，因此 WTP 没有说谎。此外，在固件下载处理期间，CAPWAP 协议没有提供任何机制去识别 WTP 是否实际上保存该固件以备将来使用。

第 13 章 运行考虑

CAPWAP 协议假设仅在到 WTP 的配置接口上配置在本 CAPWAP 规范中规定的参数。虽然独立的管理协议**可以**直接用于监控 WTP，但是不建议通过独立的管理接口配置 WTP。通过独立协议，诸如通过命令行接口(Command Line Interface, CLI)或简单网络管理协议(Simple Network Management Protocol, SNMP)，配置 WTP，可能导致 AC 状态与 WTP 不同步。

CAPWAP 协议不处理 ACs 管理。假设经由每个独立管理接口配置 AC，可能通过专用 CLI，SNMP，网络配置协议(Network Configuration Protocol, NETCONF)，或某个其他管理协议。

从流量角度看，CAPWAP 协议的控制通道十分轻便。一旦配置好 WTP，WTP 将定期发送统计数据。此外，本规范要求在协议的数据通道上发送保持激活分组，以便确信任何可能的中间体(例如，NAT)维护它们的 UDP 状态。预计与控制和数据通道有关的开销不会影响网络流量。也就是说，CAPWAP 协议考虑到经由 DataChannelKeepAlive 和 StatisticsTimer 修改这些分组的频繁程度(分别参阅第 4-7-2 节和第 4-7-14 节)。

第 14 章　传输考虑

CAPWAP WG 仔细考虑了针对 CAPWAP Control 通道和 Data 通道的 CAPWAP 协议拥塞控制要求。

CAPWAP 规定了在控制通道上使用的单线程指令/响应协议，我们规定了重复发送指令时应当使用的指数回退算法。当 CAPWAP 运行在它的默认模式时(Local MAC)，控制通道是唯一的 CAPWAP 通道。

然而，CAPWAP 也可以采用 Split MAC 模式运行，这时每个 WTP 和 AC 间将有 DTLS 的加密数据通道。为提供这个通道上的拥塞控制，WG 讨论了各种选择。然而，由于当 TCP 运行在另一个拥塞控制机制上引起的 TCP 性能问题，以及由于事实上运行在 CAPWAP Data 通道上的巨大流量极有可能是拥塞受控的 IP 流量，CAPWAP WG 相信为 CAPWAP Data 通道规定拥塞控制机制，将更有可能导致比解决任何问题更多的问题。

因为没有为 CAPWAP Data 通道规定拥塞控制机制，**建议**不要在 CAPWAP 上隧道化无拥塞控制流量。当预期大量无拥塞控制流量出现在 WLAN 上时，WLAN 的 AC 和 WTP 间的 CAPWAP 连接应当被配置为维持 Local MAC 模式，并且该模式要在 WTP 带 Distribution 功能。

CAPWAP 协议控制通道的锁步性质会使固件下载流程花费一些时间，取决于往返时间(round-trip time, RTT)。不认为这是个问题，因为当 WTP 向无线客户端/设备提供服务时，CAPWAP 协议允许下载固件。

WTP 和 AC 必须能够根据路径能力配置它们的 MTU 。更多介绍参阅第 3-5 节。借助名为“有限功能选项”的操作模式，CAPWAP 协议授权支持显式拥塞通知(Explicit Congestion Notification, ECN)，详细介绍参阅[RFC3168]第 9-1-1 节。将来的 CAPWAP 协议版本应当考虑授权支持“全部功能选项”。

第 15 章　IANA 考虑

这一章介绍 IANA 为准备发布本规范所作的工作。已经创建大量注册，包括下面的内容、文档操作(参阅[RFC5226])以及注册格式。注意位字段被引用情况，位的编码是从左到右，将最左边位标记为位 0。

对于将来的注册申请(需要 Expert Review)，应咨询 Designated Expert，Designated Expert 由负责的 IESG Area Director 任命。这样做的意图是任何分配都伴随发布 RFC，但是鉴于其他 SDOs 可能希望在 CAPWAP 上层建立内置标准，Designated Expert 可以审阅文档也是可

以接受的。在批准文档发布前，IANA 应当考虑值的分配，所以，一旦发布看来即将发生，Designated Expert 可以批准分配。Designated Expert 将向 CAPWAP WG 邮件列表(或由 Area Director 指定的替代者)发送请求，请求评论和审查。在 30 天的评审周期到期前，Designated Expert 将批准或拒绝该注册请求，并发布决定通知 CAPWAP WG 邮件列表或它的替代者，也将通知 IANA。拒绝通知必须有合理解释，有时，应当提供关于如何修改请求以便使其可以获得通过的具体建议。

15-1 IPv4 多播地址

IANA 已经根据 Internetwork Control Block IPv4 多播地址注册表，注册了称为“capwap-ac”的新 IPv4 多播地址；参阅第 3-3 节。

15-2 IPv6 多播地址

IANA 已经在 Variable Scope IPv6 多播地址注册表中，注册了称为“All ACs 多播地址”的新的组织本地多播地址；参阅第 3-3 节。

15-3 UDP端口

IANA在已注册端口号注册表中，注册了2个新UDP端口，它们是组织本地多播地址；参阅第3-1节。下述值已经注册：

Keyword	Decima	Description	References
capwap-control	5246/udp	CAPWAP Control Protocol	这个文档
capwap-data	5247/udp	CAPWAP Data Protocol	这个文档

15-4 CAPWAP 消息类型

CAPWAP Header(参阅第 4-5-1-1 节)的 Message Type 字段用于标识由该消息执行的操作。有多个命名空间，它们由包含 IANA Enterprise Number [RFC5226]的字段的前 3 个八位位组标识。

IANA 为其 Enterprise Number 设置为 0 的所有消息类型维持 CAPWAP Message Types 注册。命名空间为 8 位(0-255)，其中值 0 保留，不能分配。值 1 到值 26 在这个规范中分配，详细内容参阅第 4-5-1-1 节。新分配任何其 Enterprise Number 值设置为 0 的 CAPWAP Message Type 需要 Expert Review。由 IANA 维护的注册表格式如下：

CAPWAP Control Message	Message Type Value	Reference

15-5 CAPWAP 首部标记

在 CAPWAP Header(参阅第 4-3 节)中的 Flags 字段有 9 位长，用于标识与该消息有关的任何特殊处理。本规范定义位 0 到位 5，位 6 到位 8 保留。目前有 3 个位没有使用，所保留的位由 IANA 管理，它们的分配需要 Expert Review。IANA 建有 CAPWAP Header Flags 注册表，其格式如下：

Flag Field Name	Bit Position	Reference

15-6 CAPWAP 控制消息标记

CAPWAP Control Message 首部(参阅第 4-5-1-4 节)中的 Flags 字段用于标识与该控制消息有关的任何特殊处理。目前有 8 位没有使用，作为保留位。这些位的分配由 IANA 管理，它们的分配需要 Expert Review。IANA 建有 CAPWAP Control Message Flags 注册表，其格

式如下：

Flag Field Name　　Bit Position　　Reference

15-7　CAPWAP 消息要素类型

CAPWAP Message Element 首部(参阅第 4-6 节)中的 Type 字段用于标识发送的数据。命名空间为 16 位(0-65535)，值 0 保留，不能分配。值 1 到值 53 由本规范分配，参阅第 4-5-1-1 节。此 16 位命名空间进一步划分成地址块，用于特定 CAPWAP 无线绑定。下述块保留：

CAPWAP Protocol Message Elements	1 - 1023
IEEE 802.11 Message Elements	1024 - 2047
EPCGlobal Message Elements	3072 - 4095

这个命名空间由 IANA 管理，分配时需要 Expert Review。IANA 建有 CAPWAP Message Element Type 注册表，其格式如下：

CAPWAP Message Element　　Type Value　　Reference

15-8　CAPWAP 无线绑定标识符

CAPWAP Header(参阅第 4-3 节)中的 Wireless Binding Identifier (WBID)字段用于标识与该分组关联的无线技术。由本规范分配的值为 1、2 和 3。由于可用地址空间有限，新的 WBID 请求需要 Expert Review。IANA 建有 CAPWAP Wireless Binding Identifier 注册表，其格式如下：

CAPWAP Wireless Binding　　Identifier Type Value　　Reference

15-9　AC 安全类型

AC Descriptor 消息要素(参阅第 4-6-1 节)中的 Security 字段有 8 位长，用于标识 AC 中可用的认证方法。本规范定义位 5 和位 6，位 0 到位 4 以及位 7 保留，没有使用。这些保留位由 IANA 管理，它们的分配需要 Standards Action。IANA 建有 AC Security Types 注册表，其格式如下：

AC Security Type　　Bit Position　　Reference

15-10　AC DTLS策略

AC Descriptor消息要素(参阅第4-6-1节)中的DTLS Policy字段有8位长，用于标识是否保护CAPWAP Data Channel。本规范定义位5和位6，位0到位4以及位7保留，没有使用。这些保留位由IANA管理，分配需要Standards Action。IANA建有AC DTLS Policy注册表，其格式如下：

AC DTLS Policy　　Bit Position　　Reference

15-11　AC信息类型

AC Descriptor消息要素(参阅第4-6-1节)中的Information Type字段用于表示AC的相关信息。命名空间为16位(0-65535)，其中值0保留，不能分配。这个字段，与AC Information Vendor ID结合使用，允许供应商使用私有命名空间。本规范定义当AC Information Vendor ID设置为0时的AC Information Type命名空间，命名空间的位4和位5由本规范分配，详细介绍参阅第4-6-1节。这个命名空间由IANA管理，分配需要Expert Review。IANA建有AC Information Type注册表，其格式如下：

AC Information Type　　Type Value　　Reference

15-12　CAPWAP传输协议类型

CAPWAP Transport Protocol消息要素(参阅第4-6-14节)中的Transport字段用于标识CAPWAP Data Channel使用的传输。其命名空间为8位(0-255)，值0保留，不能使用。值1和值2由本规范分配，详细介绍参阅第4-6-14节。这个命名空间由IANA管理，分配需要Expert Review。IANA建有CAPWAP Transport Protocol Types注册表，其格式如下：

CAPWAP Transport Protocol Type　　Type Value　　Reference

15-13　数据传送类型

Data Transfer Data消息要素(参阅第4-6-15节)和Image Data信息要素(参阅第4-6-26节)中的Data Type字段，用于提供有关被携带数据的信息。命名空间为8位(0-255)，值0保留，不能使用。值1、值2和值5由本规范分配，详细介绍参阅第4-6-15节。这个命名空间由IANA管理，分配需要Expert Review。IANA建有Data Transfer Type注册表，其格式如下：

Data Transfer Type　　Type Value　　Reference

15-14　数据传送模式

Data Transfer Data 消息要素(参阅第 4-6-15 节)和 Data Transfer Mode 消息要素(参阅第 15-14 节)中的 Data Mode 字段用于提供有关被携带数据的信息。命名空间为 8 位(0-255)，值 0 保留，不能分配。值 1 和值 2 由本规范分配，详细介绍参阅第 15-14 节。这个命名空间由 IANA 管理，分配需要 Expert Review。IANA 建有 Data Transfer Mode 注册表，其格式如下：

Data Transfer Mode　　Type Value　　Reference

15-15　发现类型

Discovery Type 消息要素(参阅第 4-6-21 节)中的 Discovery Type 字段由 WTP 用于告诉 AC 怎样才能发现自己。命名空间为 8 位(0-255)。值 0 到值 4 由本规范分配，详细介绍参阅第 4-6-21 节。这个命名空间由 IANA 管理，分配需要 Expert Review。IANA 建有 Discovery Types 注册表，其格式如下：

Discovery Types　　Type Value　　Reference

15-16　ECN 支持

ECN Support 消息要素(参阅第 4-6-25 节)中的 ECN Support 字段由 WTP 用于表示它的 ECN Support。命名空间为 8 位(0-255)。值 0 和值 1 由本规范分配，详细介绍参阅第 4-6-25 节。这个命名空间由 IANA 管理，分配需要 Expert Review。IANA 建有 ECN Support 注册表，其格式如下：

ECN Support　　Type Value　　Reference

15-17　无线电设备管理状态

Radio Administrative State 消息要素(参阅第 4-6-33 节)中的 Radio Admin 字段由 WTP 用于表示它的无线电设备的状态。命名空间为 8 位(0-255)，值 0 保留，不能分配。值 1 和值 2 由本规范分配，详细介绍参阅第 4-6-33 节。这个命名空间由 IANA 管理，分配需要 Expert Review。IANA 建有 Radio Admin State 注册表，其格式如下：

Radio Admin State　　Type Value　　Reference

15-18　无线电设备运行状态

Radio Operational State消息要素(参阅第4-6-34节)中的State字段由WTP用于表示它的无

线电设备的运行状态。命名空间为8位(0-255)，值0保留，不能分配。值1和值2由本规范分配，详细介绍参阅第4-6-34节。这个命名空间由IANA管理，分配需要Expert Review。IANA建有Radio Operational State注册表，其格式如下：

Radio Operational State	Type Value	Reference

15-19　无线电设备故障原因

Radio Operational State消息要素(参阅第4-6-34节)中的Cause字段由WTP用于指出无线电设备故障原因。命名空间为8位(0-255)，值0到值3由本规范分配，详细介绍参阅第4-6-34节。这个命名空间由IANA管理，分配需要Expert Review。IANA建有Radio Failure Causes注册表，其格式如下：

Radio Failure Causes	Type Value	Reference

15-20　结果代码

Result Code消息要素(参阅第4-6-35节)中的Result Code字段用于指出CAPWAP Control消息是成功还是失败。命名空间为32位(0-4294967295)，其中值0到值22由本规范分配，详细介绍参阅第4-6-35节。这个命名空间由IANA管理，分配需要Expert Review。IANA建有Result Code注册表，其格式如下：

Result Code	Type Value	Reference

15-21　返回的消息要素原因

Returned Message Element消息要素(参阅第4-6-36节)中的Reason字段用于指出消息要素没有被成功处理的原因。命名空间为8位(0-255)，其中值0保留，不能分配。值1到值4由本规范分配，详细介绍参阅第4-6-36节。这个命名空间由IANA管理，分配需要Expert Review。IANA建有Returned Message Element Reason注册表，其格式如下：

Returned Message Element Reason	Type Value	Reference

15-22　WTP主板数据类型

WTP Board Data消息要素(参阅第4-6-40节)中的Board Data Type字段用于指出有关WTP硬件的信息。命名空间为16位(0-65535)。WTP Board Data Type值0到值4由本规范分配，详细介绍参阅第4-6-40节。这个命名空间由IANA管理，分配需要Expert Review。IANA建有WTP Board Data Type注册表，其格式如下：

WTP Board Data Type	Type Value	Reference

15-23　WTP描述符类型

WTP Descriptor消息要素(参阅第4-6-4节)中的Descriptor Type字段用于指出有关WTP软件的信息。命名空间为16位(0-65535)。这个字段，与Descriptor Vendor ID结合，使供应商能够使用私有命名空间。本规范定义当Descriptor Vendor ID 设置为0时的WTP Descriptor Type命名空间，命名空间的值0到值3由本规范分配，详细介绍参阅第4-6-41节。这个命名空间由IANA管理，分配需要Expert Review。IANA建有WTP Board Data Type（译注：此处“WTP Board Data Type”是否应换为“WTP Descriptor Type”？）注册表，其格式如下：

WTP Descriptor Type	Type Value	Reference

15-24　WTP回退模式

WTP Fallback消息要素(参阅第4-6-42节)中的Mode字段用于指出WTP应当使用的AC回

退机制类型。命名空间为8位(0-255)，值0保留，不能分配。值1和值2由本规范分配，详细介绍参阅第4-6-42节。这个命名空间由IANA管理，分配需要Expert Review。IANA建有WTP Fallback Mode注册表，其格式如下：

WTP Fallback Mode	Type Value	Reference

15-25　WTP帧隧道模式

WTP Frame Tunnel Mode消息要素(参阅第4-6-43节)中的Tunnel Type字段有8位，用于指出WTP和AC间使用的隧道化的类型。本规范定义位4到位6，位0到位3以及位7保留，不使用。这些保留的位由IANA管理，分配需要Expert Review。IANA建有WTP Frame Tunnel Mode注册表，其格式如下：

WTP Frame Tunnel Mode	Bit Position	Reference

15-26　WTP MAC类型

WTP MAC Type消息要素(参阅第4-6-44节)中的MAC Type字段用于指出在WTP和AC间隧道化帧中使用的MAC类型。命名空间为8位(0-255)，值0到值2由本规范分配，详细介绍参阅第4-6-44节。这个命名空间由IANA管理，分配需要Expert Review。IANA建有WTP MAC Type注册表，其格式如下：

WTP MAC Type	Type Value	Reference

15-27　WTP无线电设备统计量故障类型

WTP Radio Statistics消息要素(参阅第4-6-46节)中的Last Failure Type字段用于指出上一次WTP故障。命名空间为8位(0-255)，值0到值3，以及值255由本规范分配，详细介绍参阅第4-6-46节。这个命名空间由IANA管理，分配需要Expert Review。IANA建有WTP Radio Stats Failure Type注册表，其格式如下：

WTP Radio Stats Failure Type	Type Value	Reference

15-28　WTP 重启统计量故障类型

WTP Reboot Statistics 消息要素(参阅第 4-6-47 节)中的 Last Failure Type 字段用于指出上一次重启原因。命名空间为 8 位(0-255)，值 0 到值 5，以及值 255 由本规范分配，详细介绍参阅第 4-6-47 节。这个命名空间由 IANA 管理，分配需要 Expert Review。IANA 建有 WTP Reboot Stats Failure Type 注册表，其格式如下：

WTP Reboot Stats Failure Type	Type Value	Reference

第16章　致谢

下述人士为本协议规范作出了贡献，在此一并感谢：

Puneet Agarwal、Abhijit Choudhury、Pasi Eronen、Saravanan Govindan、Peter Nilsson、David Perkins和Yong Zhang。Michael Vakulenko对CAPWAP怎样才能在第3层网络(IP/UDP)上使用给出了文字说明。

第17章　参考文献

17-1　标准类参考文献

[RFC1191]　Mogul, J. and S. Deering, "Path MTU discovery", RFC 1191, November 1990.

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[RFC1305] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation", RFC 1305, March 1992.

[RFC1981] McCann, J., Deering, S., and J. Mogul, "Path MTU Discovery for IP version 6", RFC 1981, August 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, September 2001.

[RFC3539] Aboba, B. and J. Wood, "Authentication, Authorization and Accounting (AAA) Transport Profile", RFC 3539, June 2003.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

[RFC3828] Larzon, L-A., Degermark, M., Pink, S., Jonsson, L-E., and G. Fairhurst, "The Lightweight User Datagram Protocol (UDP-Lite)", RFC 3828, July 2004.

[RFC4086] Eastlake, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

[RFC4279] Eronen, P. and H. Tschofenig, "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279, December 2005.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC4347 Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 2006.

[RFC4821] Mathis, M. and J. Heffner, "Packetization Layer Path MTU Discovery", RFC 4821, March 2007.

[RFC4963] Heffner, J., Mathis, M., and B. Chandler, "IPv4 Reassembly Errors at High Data Rates", RFC 4963, July 2007.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[ISO.9834-1.1993] International Organization for Standardization, "Procedures for the operation of OSI registration authorities - part 1: general procedures", ISO Standard 9834-1, 1993.

[RFC5416] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed.,

"Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11", RFC 5416, March 2009.

[RFC5417] Calhoun, P., "Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option", RFC 5417, March 2009.

[FRAME-EXT] IEEE, "IEEE Standard 802.3as-2006", 2005.

17-2 信息类参考文献

[RFC3232] Reynolds, J., "Assigned Numbers: RFC 1700 is Replaced by an On-line Database", RFC 3232, January 2002.

[RFC3753] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[RFC4564] Govindan, S., Cheng, H., Yao, ZH., Zhou, WH., and L. Yang, "Objectives for Control and Provisioning of Wireless Access Points (CAPWAP)", RFC 4564, July 2006.

[RFC4962] Housley, R. and B. Aboba, "Guidance for Authentication, Authorization, and Accounting (AAA) Key Management", BCP 132, RFC 4962, July 2007.

[LWAPP] Calhoun, P., O'Hara, B., Suri, R., Cam Winget, N., Kelly, S., Williams, M., and S. Hares, "Lightweight Access Point Protocol", Work in Progress, March 2007.

[SLAPP] Narasimhan, P., Harkins, D., and S. Ponnuswamy, "SLAPP: Secure Light Access Point Protocol", Work in Progress, May 2005.

[DTLS-DESIGN] Modadugu, et al., N., "The Design and Implementation of Datagram TLS", Feb 2004.

[EUI-48] IEEE, "Guidelines for use of a 48-bit Extended Unique Identifier", Dec 2005.

[EUI-64] IEEE, "GUIDELINES FOR 64-BIT GLOBAL IDENTIFIER (EUI-64) REGISTRATION AUTHORITY".

[EPCGlobal] "See http://www.epcglobalinc.org/home".

[PacketCable] "PacketCable Security Specification PKT-SP-SECI12-050812", August 2005, <PacketCable>.

[CableLabs] "OpenCable System Security Specification OC-SPSEC-I07-061031", October 2006, <CableLabs>.

[WiMAX] "WiMAX Forum X.509 Device Certificate Profile Approved Specification V1.0.1", April 2008, <WiMAX>.

[RFC5418] Kelly, S. and C. Clancy, "Control And Provisioning for Wireless Access Points (CAPWAP) Threat Analysis for IEEE 802.11 Deployments", RFC 5418, March 2009.

编辑通讯录

Pat R. Calhoun (editor)
Cisco Systems, Inc.

170 West Tasman Drive
San Jose, CA 95134
Phone: +1 408-902-3240
EMail: pcalhoun@cisco.com

Michael P. Montemurro (editor)
Research In Motion
5090 Commerce Blvd
Mississauga, ON L4W 5M4
Canada
Phone: +1 905-629-4746 x4999
EMail: mmontemurro@rim.com

Dorothy Stanley (editor)
Aruba Networks
1322 Crossman Ave
Sunnyvale, CA 94089
Phone: +1 630-363-1389
EMail: dstanley@arubanetworks.com