CAPWAP基础原理

www.huawei.com

HUAWEI

培训目标

- 学完本课程后，您应该能：
  - 区分AP技术
  - 描述CAPWAP隧道协议

目 录

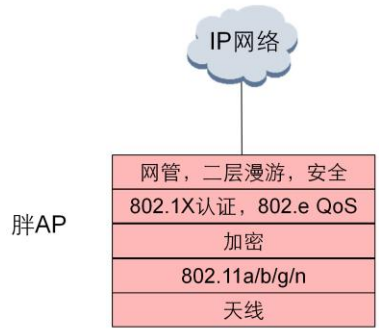
AP介绍

- 无线局域网络的架构主要分为:
  - 基于控制器的AP架构（瘦AP，Fit AP）
  - 传统的独立AP架构（胖AP，Fat AP）
- 随着近几年WLAN技术以及市场的发展，瘦AP正在迅速替代胖AP模式。

=

胖AP介绍

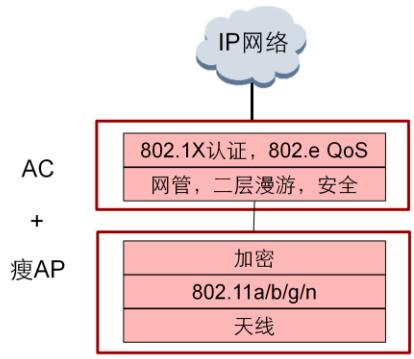
- 胖AP，除无线接入功能外，一般具备WAN、LAN两个接口，多支持DHCP服务器、DNS和MAC地址克隆，以及VPN接入、防火墙等安全功能。



- 所谓的胖AP，典型的例子为无线路由器。无线路由器与纯AP不同，除无线接入功能外，一般具备WAN、LAN两个接口，多支持DHCP服务器、DNS和MAC地址克隆，以及VPN接入、防火墙等安全功能。

瘦AP介绍

- 瘦AP是“代表自身不能单独配置或者使用的无线AP产品，这种产品仅仅是一个WLAN系统的一部分，负责管理安装和操作”。



 Page5 HUAWEI

- 对于可运营的WLAN，从组网的角度，为了实现WLAN网络的快速部署、网络设备的集中管理、精细化的用户管理，相比胖AP（自治性AP）方式，企业用户以及运营商更倾向于采用集中控制性WLAN组网（瘦AP+AC），从而实现WLAN系统、设备的可运维、可管理。
- AC和瘦AP之间运行的协议一般为CAPWAP协议。

胖AP与瘦AP比较

	AC+瘦AP	胖AP
投资	AP成本较低，易管理； AC成本高 。	AP成本较高，但是无AC投入。
WLAN组网	1. AP不能单独工作，需要由AC集中代理维护管理； 2. AP本身零配置，适合大规模组网； 3. 存在多厂商兼容性问题，AC和AP间为私有协议，必须为同厂家设备； 4. 每个AC管理AP容量较少。	1. 需要对AP下发配置文件； 2. 有网管情况下可以支持大规模网络部署和海量规模用户管理； 3. 不存在兼容性问题：基于AP和网管系统之间采用标准的IP层协议互通； 4. 网管可以实现海量AP统一集中管理和维护，并实现与现有宽带网络融合管理；
业务能力	二层、三层漫游； 可扩展语音等丰富业务； 可以通过AC增强业务QoS、安全等功能。	二层漫游； 实现简单数据接入。

目 录

CAPWAP背景

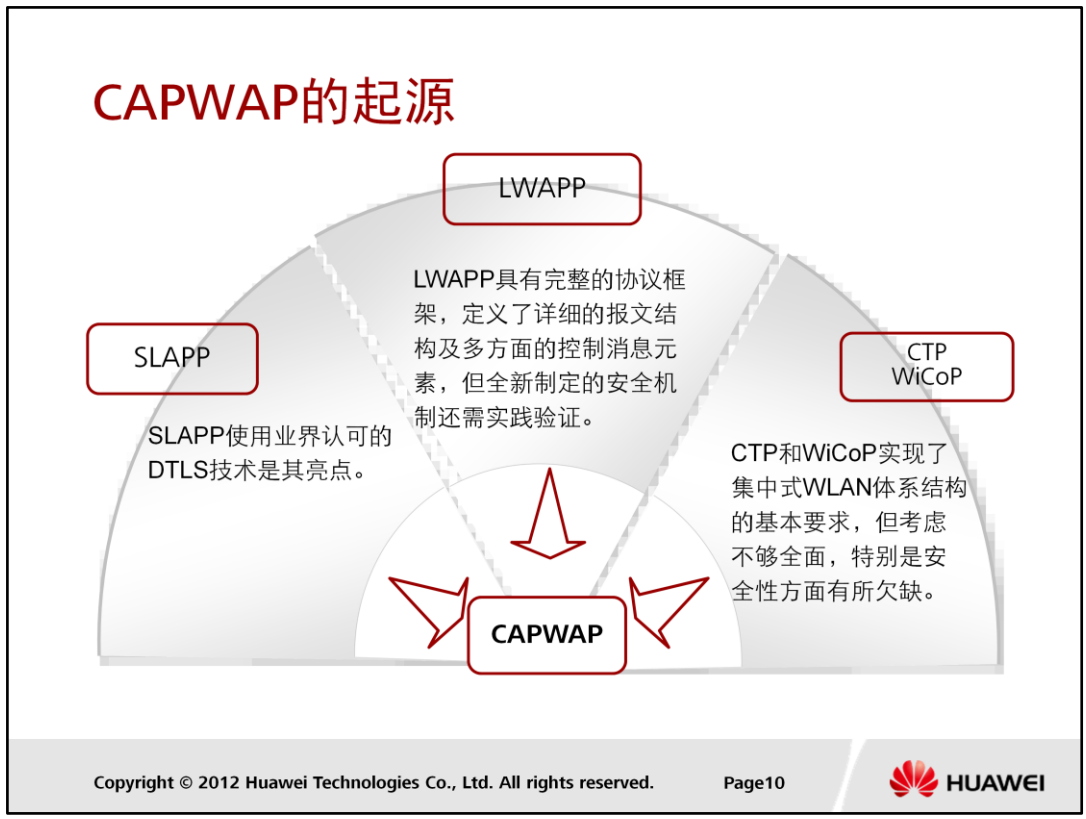
- 传统的WLAN体系结构已无法满足大规模组网需求，因此，IETF成立了CAPWAP（Control And Provisioning of Wireless Access Points）工作组，研究大规模WLAN的解决方案。以实现各个厂家控制器与AP间的互通。

  HUAWEI

- Control And Provisioning of Wireless Access Points： 无线接入点控制和配置协议

CAPWAP工作组参考了4个不同的协议

协议名称	LWAPP	SLAPP	CTP	WiCoP
标准	RFC5412	RFC5413	draft-singh-capwap-ctp	RFC5414
协议全称	Light Weight Access Point Protocol	Secure Light Access Point Protocol	CAPWAP Tunneling Protocol	Wireless LAN Control Protocol
提出厂家	Cisco - AirSpace	Aruba	Siemens - Chantry	Panasonic
协议特点	全面的描述了AC发现、安全和系统管理方法，支持本地MAC和分离MAC机制。两者连接采用2层或3层连接，2层连接使用以太网帧传输，3层连接使用UDP传输LWAPP报文	支持桥接和隧道两种本地MAC机制。支持直连、2层和3层三种连接方式。使用成熟的技术标准来建立通信隧道，数据信道使用GRE技术	利用扩展的SNMP对WTP进行配置和管理。CTP的控制消息着重于STA连接状态、WTP配置和状态几方面	定义了包括无线终端-AC性能协商功能在内的AC发现机制，定义了QoS参数
加密情况	信令 – AES-CCM 数据 – 没有加密	信令 – DTLS 数据 – DTLS	建立了AP与无线终端互相认证及一套基于AES-CCM的加密规则，但是并不完善	协议建议使用IPsec和EAP安全标准，却并未详细说明实现方法



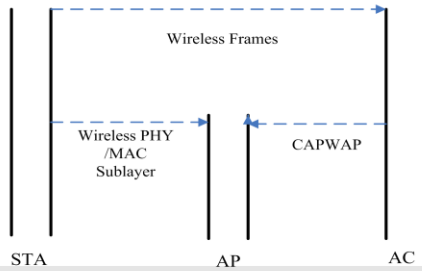
- LWAPP具有完整的协议框架，定义了详细的报文结构及多方面的控制消息元素，但全新制定的安全机制还需实践验证，而SLAPP使用业界认可的DTLS技术是其亮点。相对前两者而言，CTP和WiCoP实现了集中式WLAN体系结构的基本要求，但考虑不够全面，特别是安全性方面有所欠缺。
- CAPWAP工作组对以上四种通信协议进行评测后，最终采用LWAPP协议作为基础进行扩展，使用DTLS安全技术，加入其他三种协议的有用特性，制定了CAPWAP协议。

CAPWAP介绍

- CAPWAP（无线接入点控制和配置协议），用于无线终端接入点（AP）和无线网络控制器（AC）之间的通信交互，实现AC对其所关联的AP的集中管理和控制。
- 该协议包含的主要内容有：
  - AP对AC的自动发现及AP&AC的状态机运行、维护
  - AC对AP进行管理、业务配置下发
  - STA数据封装CAPWAP隧道进行转发

CAPWAP模式：Split MAC

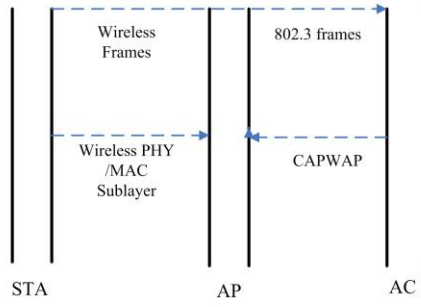
- CAPWAP协议支持两种操作模式：Split MAC和Local MAC。
- Split MAC:
  - 在Split MAC模式下，所有二层的无线数据和管理帧都被CAPWAP协议封装，在AC和AP之间交互。
  - 从STA收到的无线帧，直接封装，转发给AC,如下图：



- 在split MAC模式下，无线报文不经过报文转换，直接到达AC，

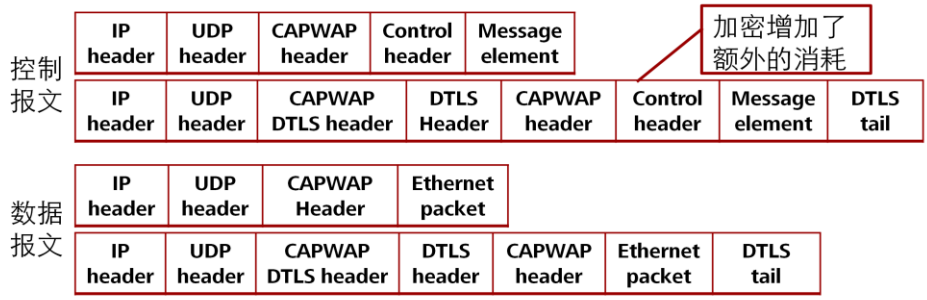
CAPWAP模式：Local MAC

- Local MAC:
  - 本地转发模式允许数据帧可以用本地桥或者使用802.3的帧形式用隧道转发。二层无线管理帧在AP本地处理，然后再转发给AC，如下图：（STA传送的无线帧在AP被封装成802.3数据帧）



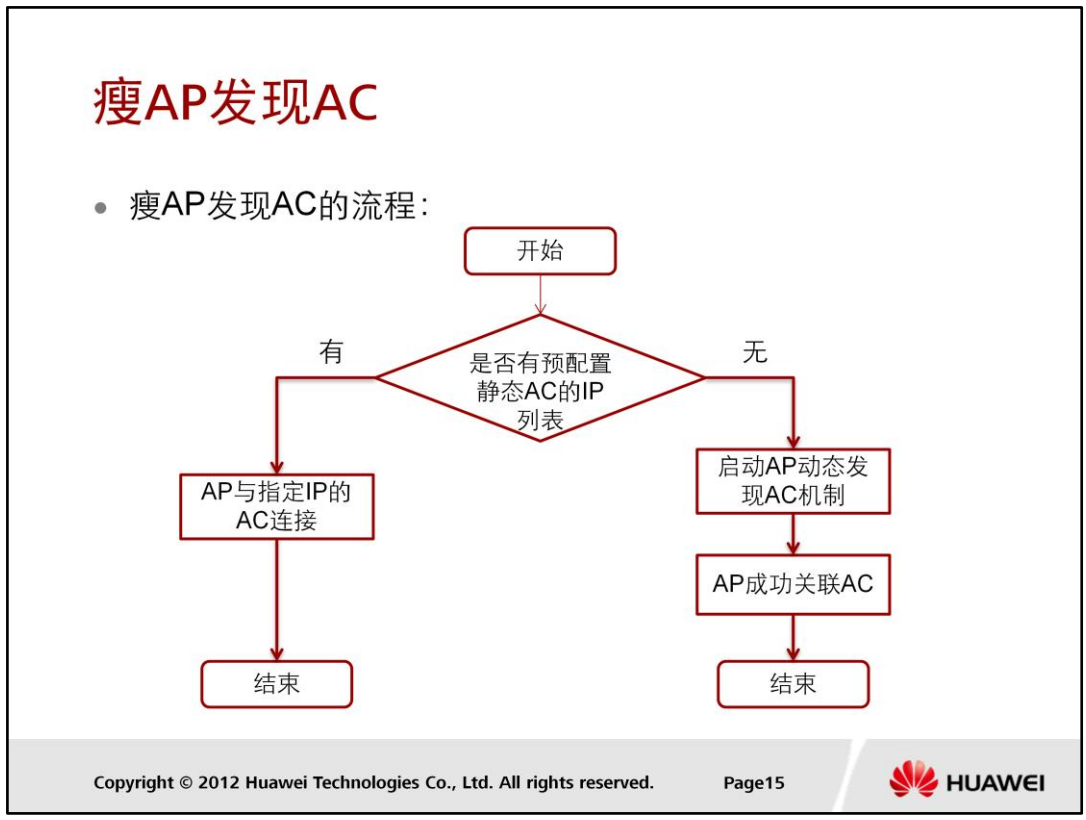
CAPWAP基本报文格式

报文类型	用于	UDP端口	加密
控制报文	管理AP	5246	大部分是密文
数据报文	转发用户数据	5247	大部分是明文



 Page14 HUAWEI

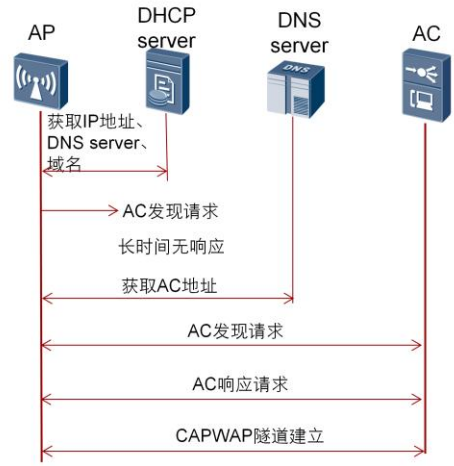
- CAPWAP是基于UDP端口的应用层协议。
- CAPWAP协议传输层运输两种类型的负载：
  - 数据消息，封装转发无线帧 。
  - 控制消息，管理AP和AC之间交换的管理消息 。
- CAPWAP数据和控制报文基于不同的UDP端口发送：
  - 控制报文端口为UDP端口5246。
  - 数据报文端口为UDP端口5247。



- AP上电后，当存在预配置的AC IP列表时，则AP直接启动预配置静态发现流程并与指定的AC连接。
- 如果未配置AC IP列表，则启动AP动态发现AC机制，执行DHCP/DNS/广播发现流程后与AC连接。

瘦AP发现AC

- 瘦AP动态发现AC的过程：



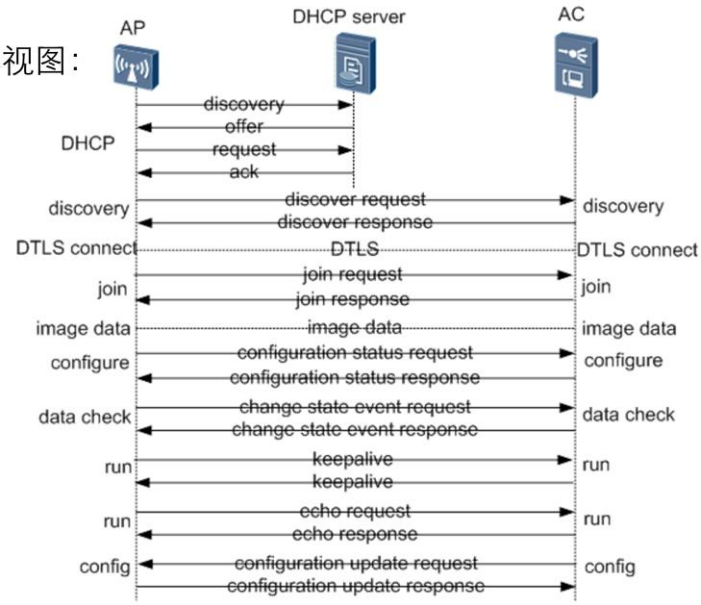
- 1、AP启动以后会通过DHCP获取IP地址、DNS server、域名。
- 2、AP发出L2广播的发现请求报文试图联系一个AC。
- 3、如果长时间（30秒）没有响应,AP会启动L3发现。AP会从DHCP Server通过Option43获得AC的IP，或者通过Option15获得AC的域名，AP向该IP地址（域名）发送发现请求。
- 4、接收到发现请求报文的AC会检查该AP是否有接入本机的权限，如果有则回应发现响应。
- 5、AC和AP间建立CAPWAP隧道。

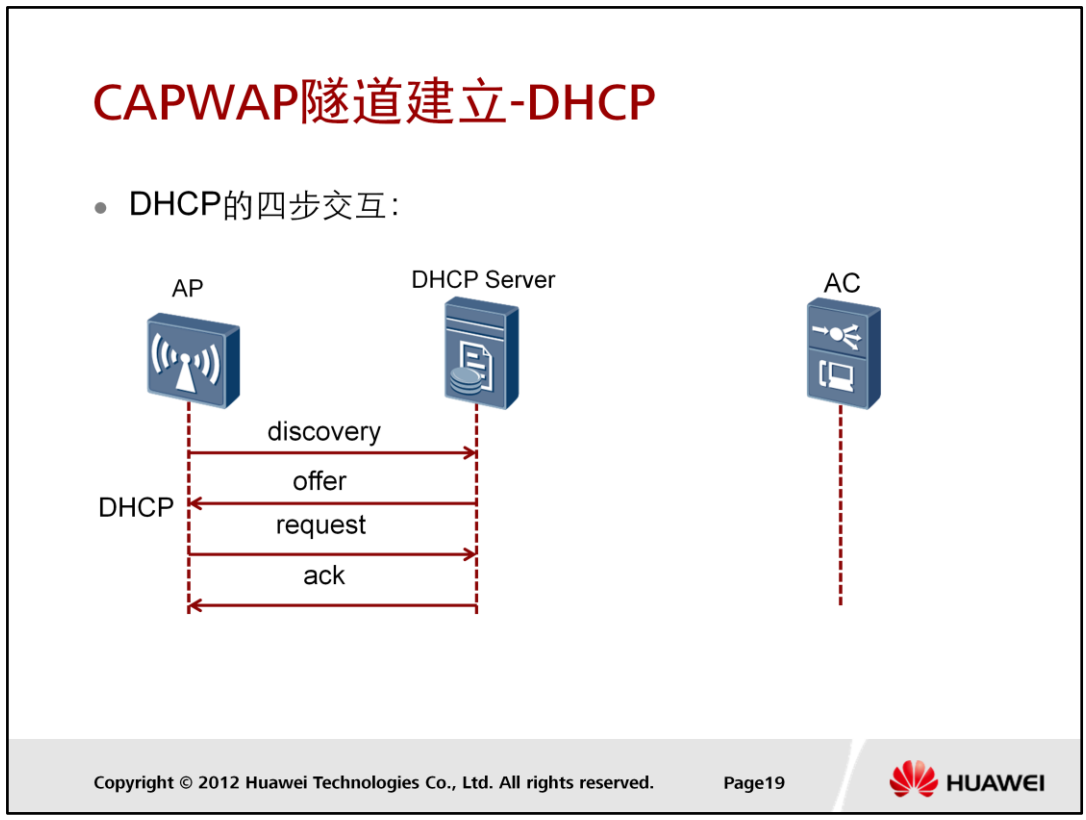
现网例外情况解决建议

- 现网DHCP server既不支持Option43，也不支持Option15，则采取以下几种措施：
  - AC与AP采用二层组网，启用CAPWAP广播发现
  - AC与AP仍用三层组网
    - 推荐使用AC自带DHCP server给AP分IP
      - AP管理流与STA业务流分不同vlan
    - 增加部署一台支持option43的DHCP server
      - 单独为AP建立一个新的DHCP server

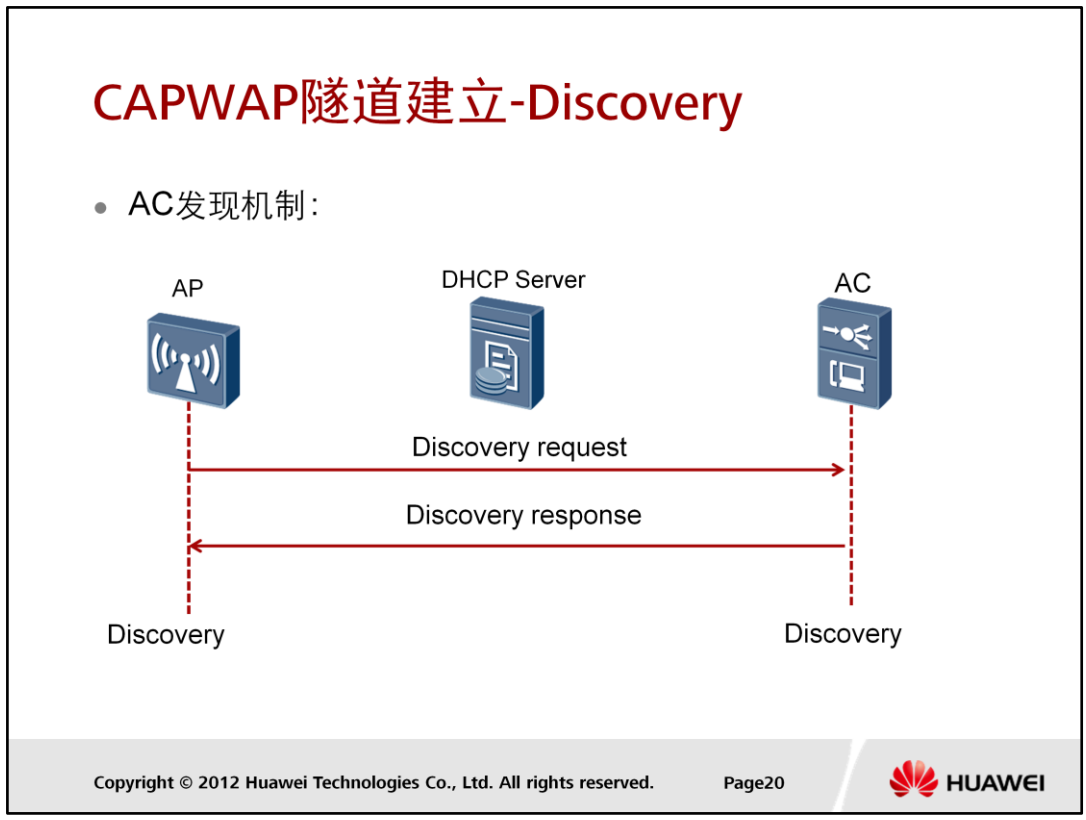
CAPWAP隧道建立

- 总体视图：

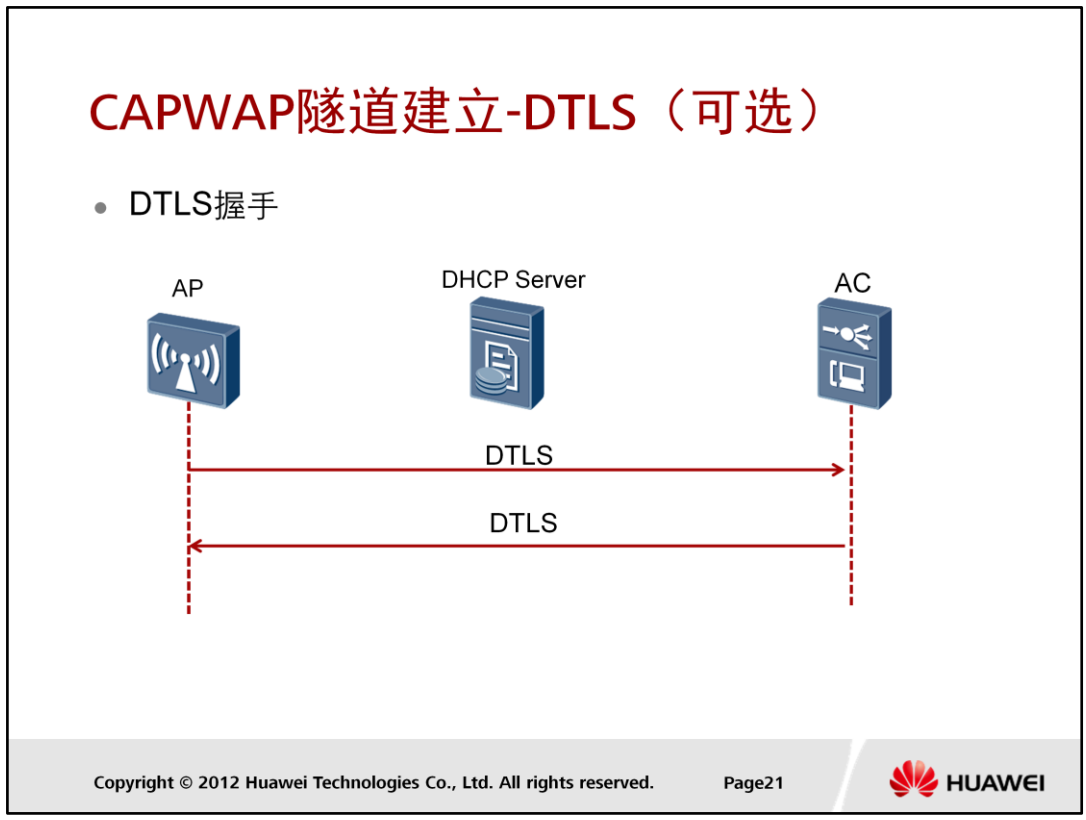




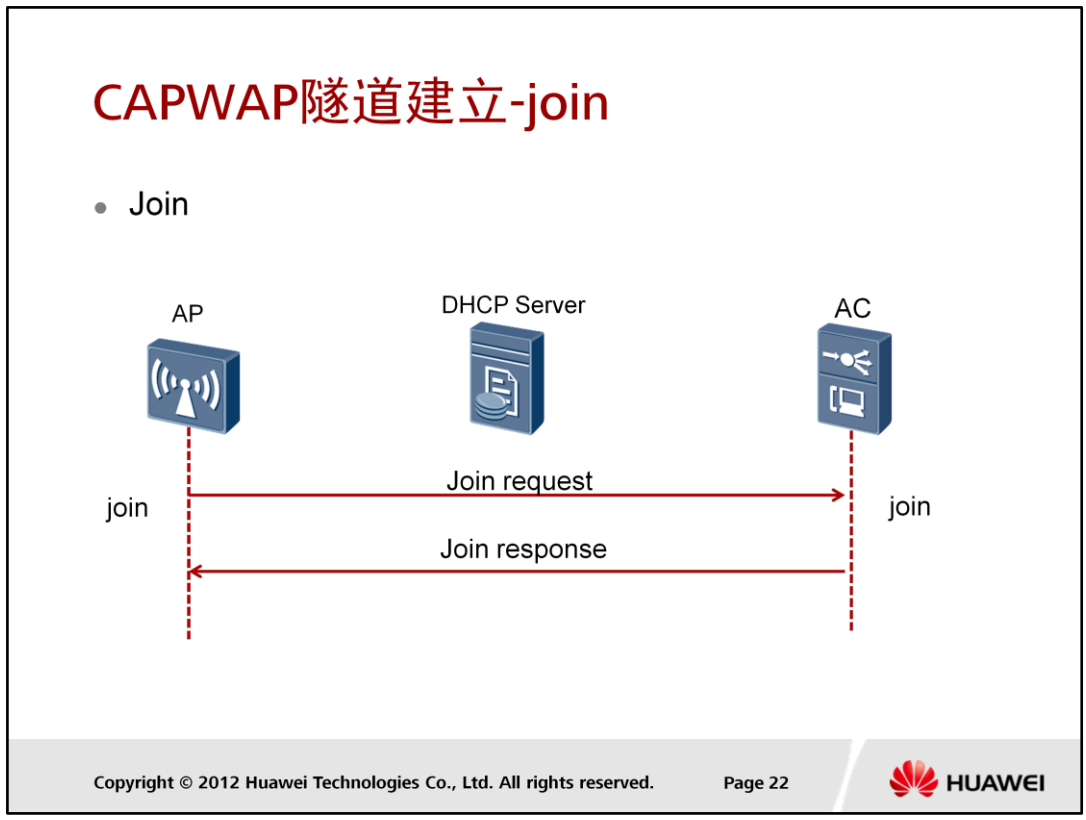
- DHCP的四步交互：
  - 在没有预配置AC IP列表时，则启动AP动态AC发现机制。通过DHCP获取IP地址，并通过DHCP协议中的option返回AC地址列表。
  - 首先是AP发送discover广播报文，请求DHCP server响应，在DHCP服务器侦听到discover报文后，它会从没有租约的地址范围中，选择最前面的空置IP，连同其他TCP/IP设定，响应AP一个DHCP offer报文，该报文中会包含一个租约期限的信息。
  - 由于DHCP offer报文既可以是单播报文，也可以是广播报文，当AP端收到多台DHCP Server的响应时，只会挑选其中一个offer(通常是最先抵达的那个)，然后向网络中发送一个DHCP request广播报文，告诉所有的offer，并重新发送DHCP，DHCP server它将指定接收哪一台服务器提供的IP地址，同时，AP也会向网络发送一个ARP封包，查询网络上面有没有其他机器使用该IP地址，如果发现该IP已被占用，AP会发送出一个DHCP Decline封包给DHCP服务器，拒绝接收其DHCP discover 报文。
  - 当DHCP Server接收到AP的request报文之后，会向AP发送一个DHCP Ack响应，该报文中携带的信息包括了AP的IP地址，租约期限，网关信息，以及DNS server IP等，以此确定租约的正式生效，就此完成DHCP的四步交互工作。



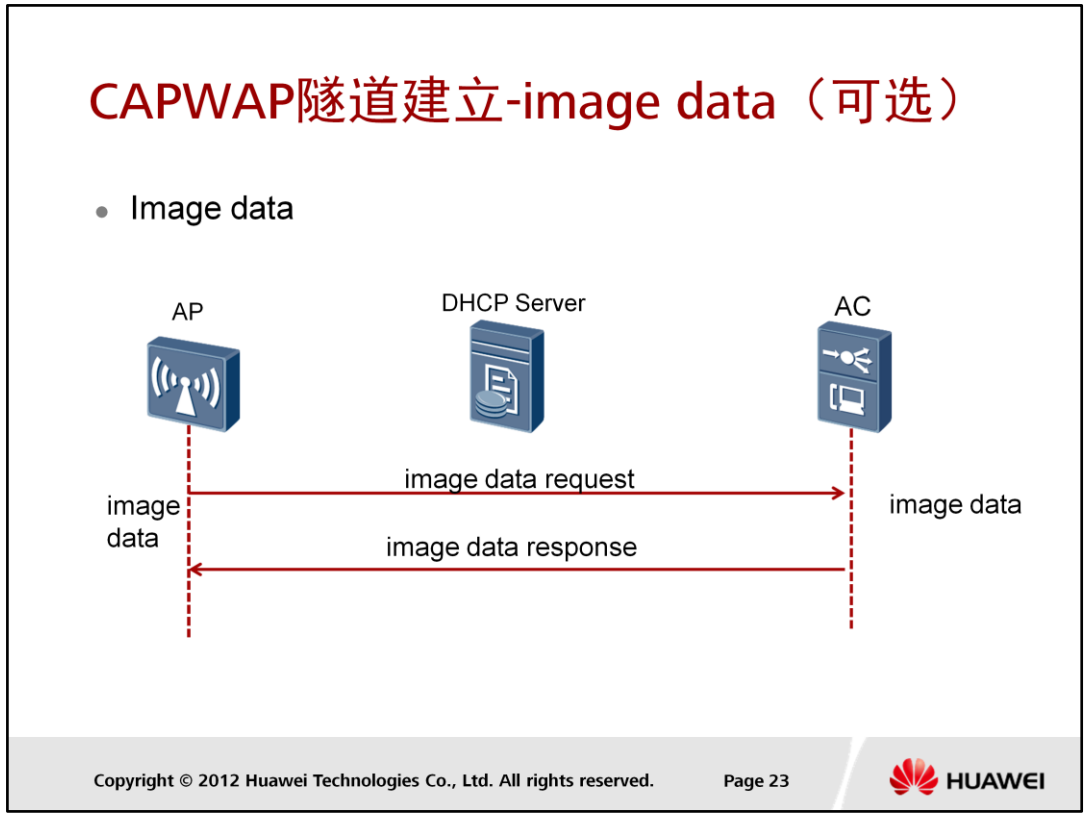
- AC发现机制：
  - AP使用AC发现机制来获知哪些AC是可用的，决定与最佳AC来建立CAPWAP的连接。（当然，AP的发现过程是可选的，如果在AP上已经静态配置了AC，那么就不需要完成AC的发现过程。）
  - AP启动CAPWAP协议的发现机制，以单播或广播的形式发送发现请求报文试图关联AC，AC收到AP的discovery request以后，会发送一个单播discover response给AP，AP可以通过discover response中所带的AC优先级或者AC上当前AP的个数等，确定与哪个AC建立会话。



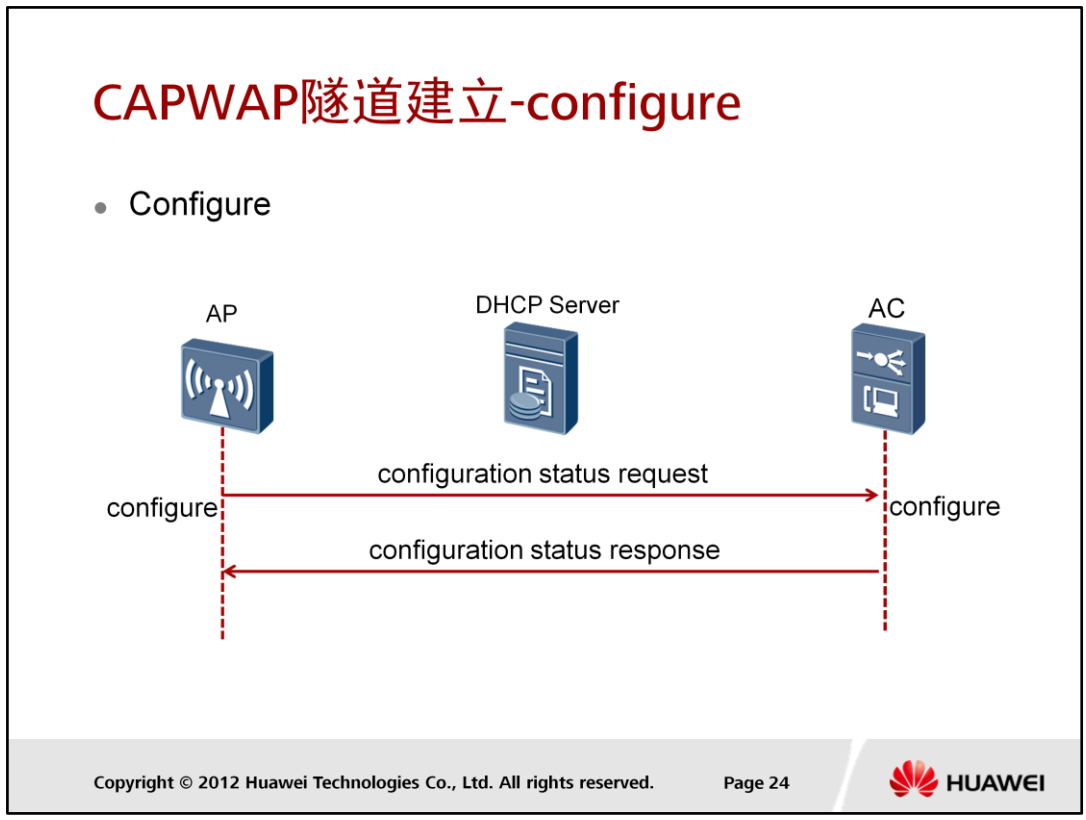
- DTLS握手：
  - AP根据此IP地址与AC协商，AP接收到响应消息后开始与AC建立CAPWAP隧道，这个阶段可以选择CAPWAP隧道是否采用DTLS加密传输UDP报文。
  - DTLS: Datagram Transport Layer Security（数据报传输层安全协议）



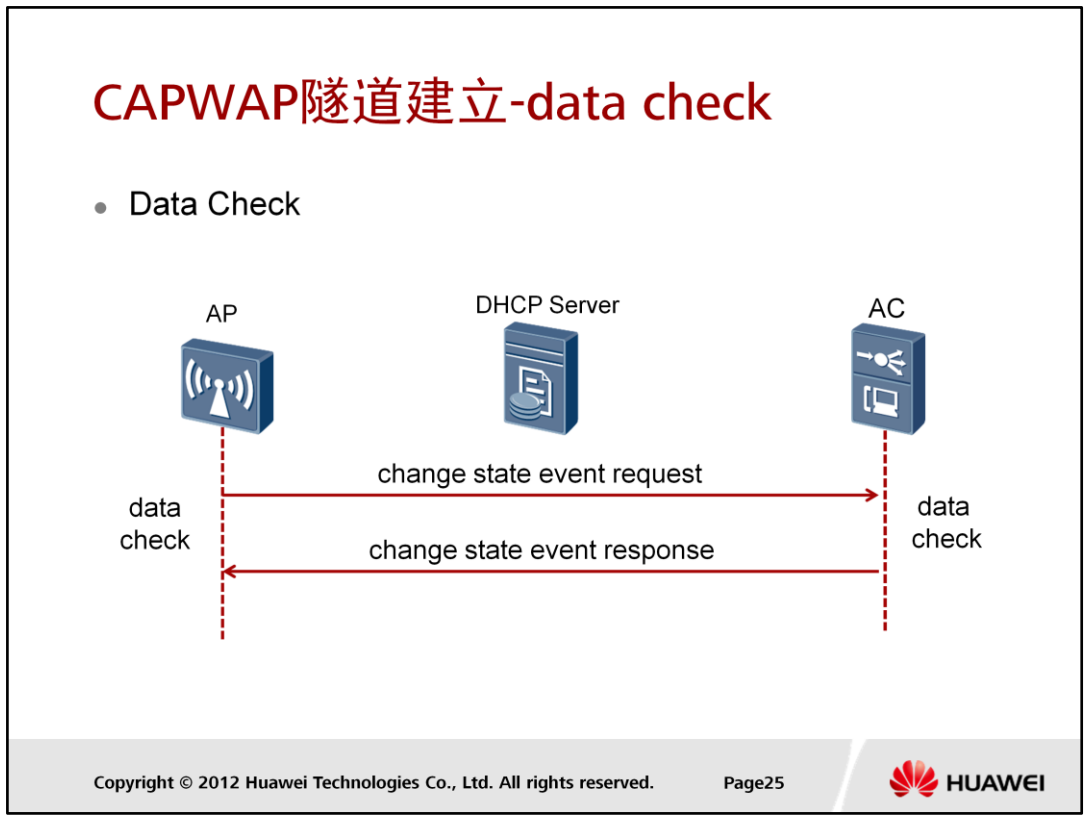
- Join：
  - 在完成DTLS握手后，AC与AP开始建立控制通道，在建立控制的交互过程中，AC回应的Join response报文中会携带用户配置的升级版本号，握手报文间隔/超时时间，控制报文优先级等信息。AC会检查AP的当前版本，如果AP的版本无法与AC要求的相匹配时，AP和AC会进入Image Data状态做固件升级，以此来更新AP的版本，如果AP的版本符合要求，则进入configuration状态。



- image data：
  - AP根据协商参数判断当前版本是否是最新版本，如果不是最新版本，则AP将在CAPWAP隧道上开始更新软件版本。
  - AP在软件版本更新完成后重新启动，重复进行AC发现、建立CAPWAP隧道、加入过程。



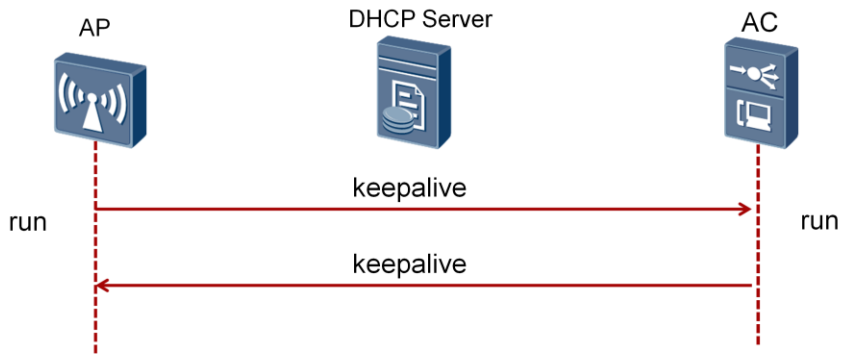
- Configuration：
  - 进入Configuration状态后是为了做AP的现有配置和AC设定配置的匹配检查，AP发送configuration request到AC，该信息中包含了现有AP的配置，当AP的当前配置与AC要求不符合时，AC会通过configuration response通知AP。



- Data Check：
  - 当完成configuration后，AP发送change state event request信息，其中包含了radio，result，code等信息，当AC接收到change state event request后，开始回应change state event response 。
- 至此完成data check 后，已经完成管理隧道建立的过程，开始进入run状态。

CAPWAP隧道维护-run（data）

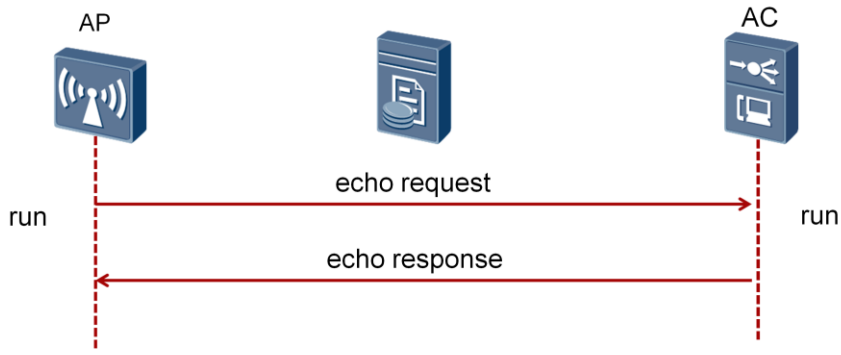
- Run（数据）



- Run：
  - AP发送keepalive到AC，AC收到keepalive后表示数据隧道建立，AC回应keepalive，AP进入“normal”状态，开始正常工作。

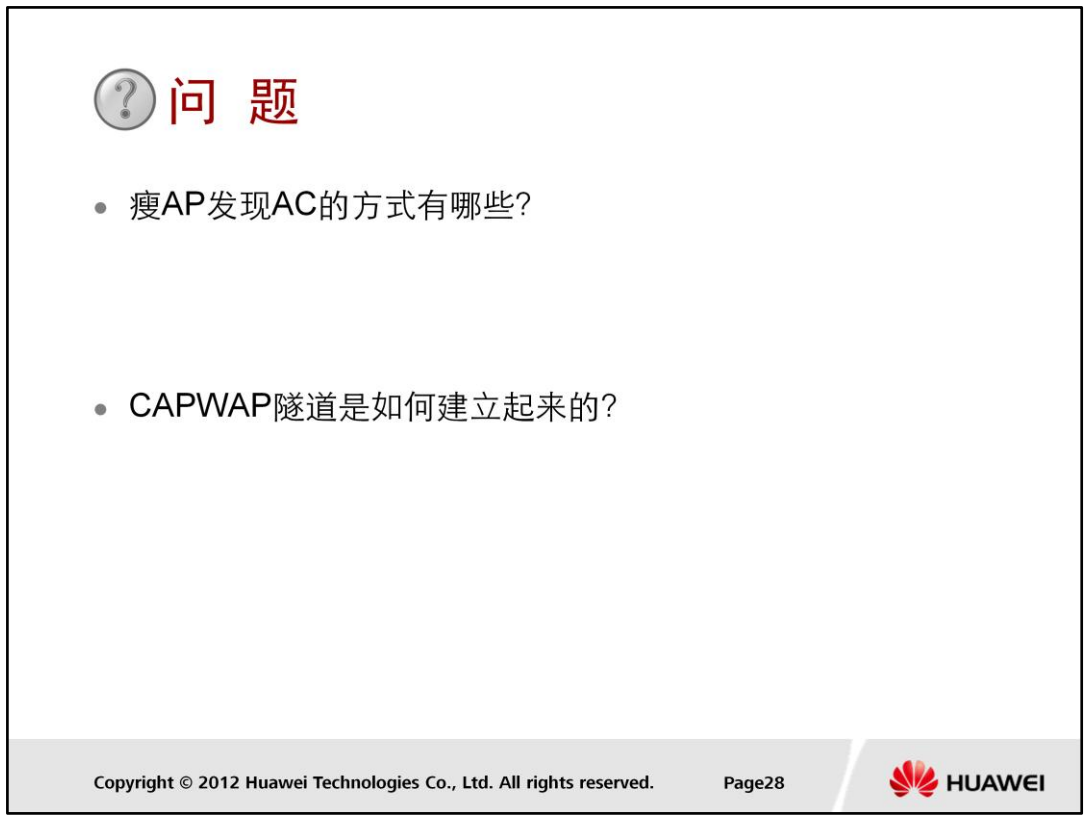
CAPWAP隧道维护-run（control）

- Run（控制）



  HUAWEI

- 管理隧道维护：
  - AP进入run状态后，同时发送echo request报文给AC，宣布建立好CAPWAP管理隧道并启动echo发送定时器和隧道检测超时定时器以检测管理隧道时候异常。
  - 当AC收到echo request报文后，同样进入run状态，并回应echo response报文给AP，启动隧道超时定时器。
  - 到AP收到echo response报文后，会重设检验隧道超时的定时器。



- 瘦AP发现AC的方式有哪些?
  - AP自动发现AC分为静态发现与动态发现。动态发现有DHCP动态发现与DNS动态发现。
- CAPWAP隧道是如何建立起来的?
  - CAPWAP隧道建立过程有:
    - Discovery阶段
    - DTLS协商阶段（可选）
    - Join阶段
    - Image data阶段（可选）
    - configure
    - Data check阶段
    - Run（Data）阶段
    - Run（Control）阶段

总 结

- 胖AP技术
- 瘦AP技术
- CAPWAP隧道的建立过程

谢谢

www.huawei.com