WLAN组网介绍

www.huawei.com

HUAWEI

培训目标

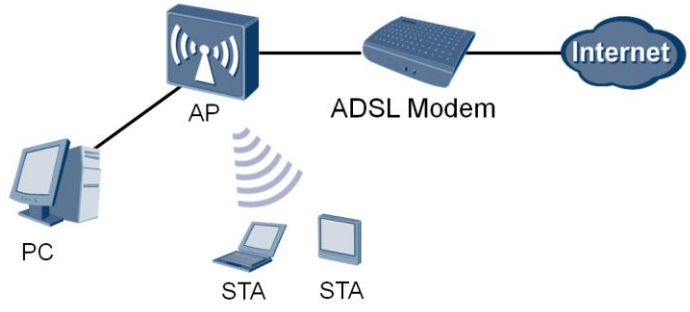
- 学完本课程后，您应该能：
  - 概括WLAN一般组网方式
  - 区分WLAN转发方式
  - 区分WLAN业务中不同VLAN的应用

HUAWEI

目 录

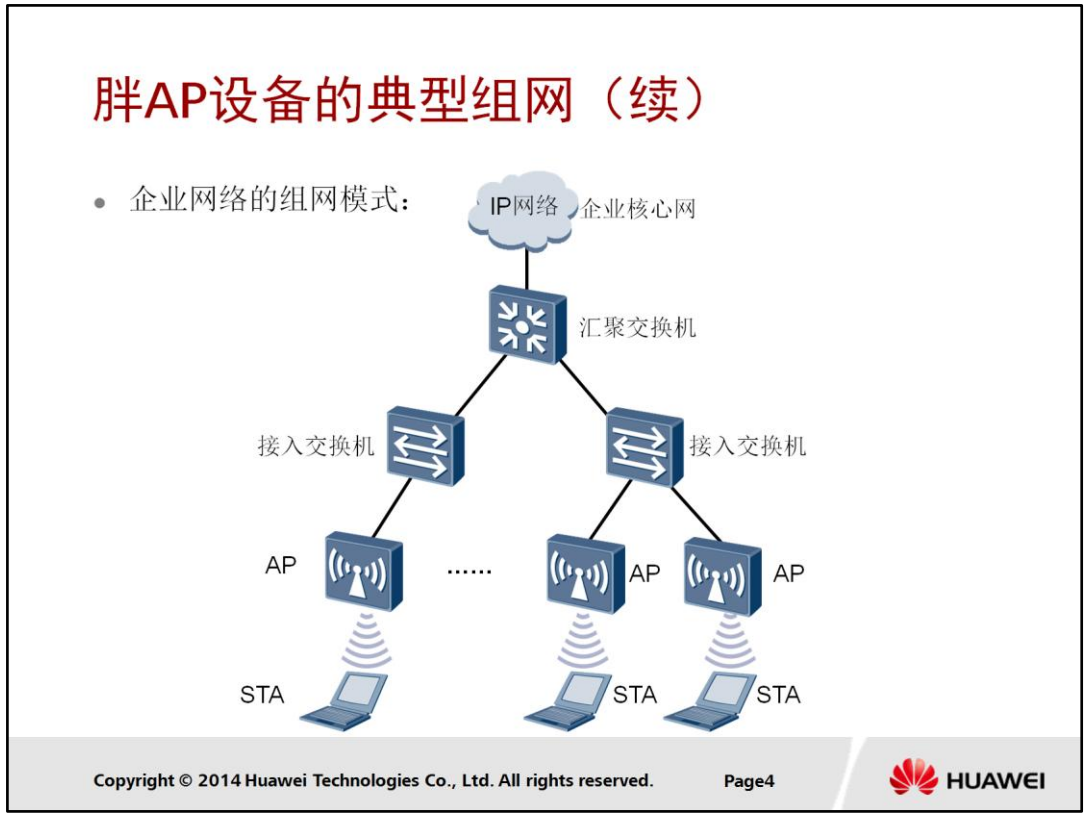
胖AP设备的典型组网

- 家庭或 soho 网络的组网模式：

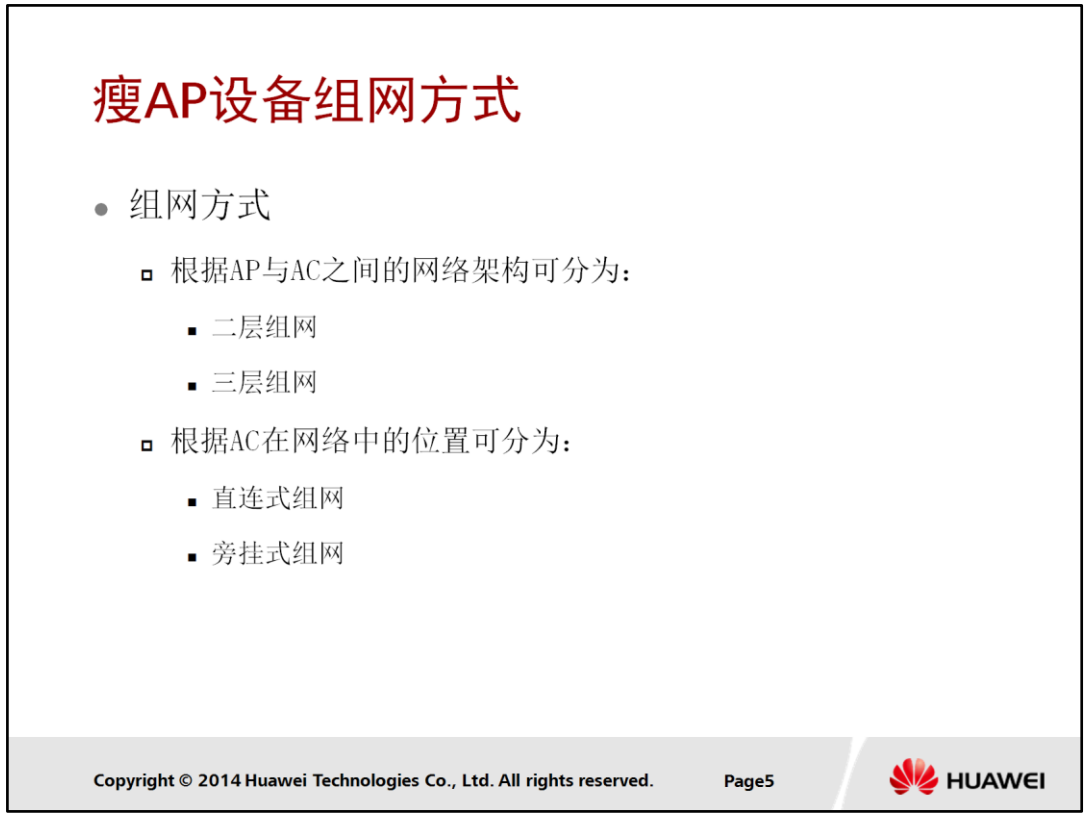


HUAWEI

- 在家庭或者SOHO中，由于所需要的无线覆盖范围小，一般采用胖AP组网。而胖AP可以不仅实现无线覆盖的要求，还可以同时作为路由器，实现对有线网络的路由转发。



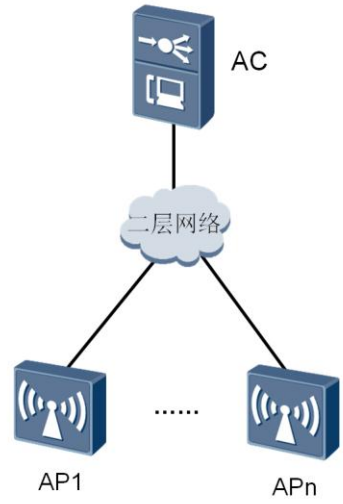
- 在企业网络或者其他大型场所中，所需要的无线覆盖范围比较大，若采用胖AP组网，则可以将AP接入到接入交换机端，数据通过交换机的转发，到达企业核心网。在企业核心网也可以架设起网管系统，便于对AP的统一管理。



- 无线控制器＋FIT AP控制架构（瘦AP）对设备的功能进行了重新划分，其中无线控制器负责无线网络的接入控制，转发和统计、AP的配置监控、漫游管理、AP的网管代理、安全控制；FIT AP负责802.11报文的加解密、802.11的物理层功能、接受无线控制器的管理、RF空口的统计等简单功能。

瘦AP设备组网方式（续）

- 二层网络连接模式
  - 瘦AP和无线控制器同属于一个二层广播域，瘦AP和AC之间通过二层交换机互联。

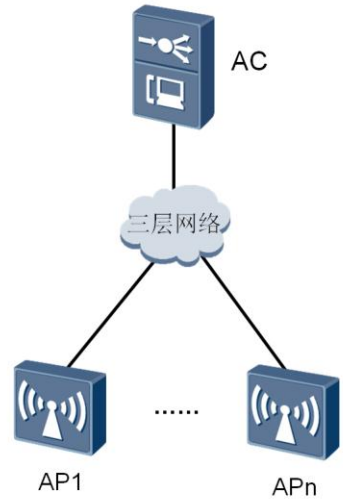


  HUAWEI

- 当AC与AP之间的网络为直连或者二层网络时，此组网方式为二层组网。
- 由于二层组网比较简单，适用于简单临时的组网，能够进行比较快速的组网配置，但不适用于大型组网架构。

瘦AP设备组网方式（续）

- 三层网络连接模式
  - 瘦AP和无线控制器属于不同的IP网段。瘦AP和AC之间的通信需要通过路由器或者三层交换机三层转发来完成。

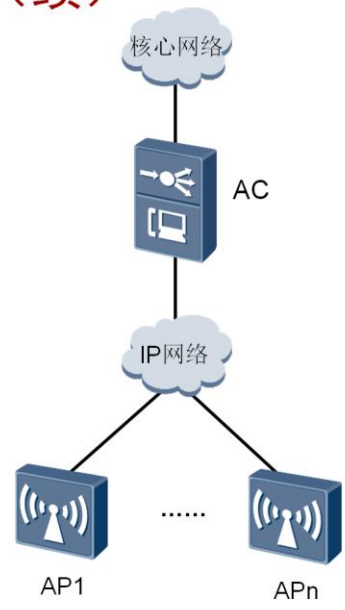


 Page7 HUAWEI

- 当AP与AC之间的网络为三层网络时，WLAN组网为三层组网。
- 在实际组网中，一台AC可以连接几十甚至几百台AP，组网一般比较复杂。比如在企业网络中，AP可以布放在办公室，会议室，会客间等场所，而AC可以安放在公司机房，这样，AP和AC之间的网络就是比较复杂的三层网络。因此，在大型组网中一般采用三层组网。

瘦AP设备组网方式（续）

- 直连式组网
  - 直连式组网中AC同时扮演AC和汇聚交换机的功能，AP的数据业务和管理业务都由AC集中转发和处理。

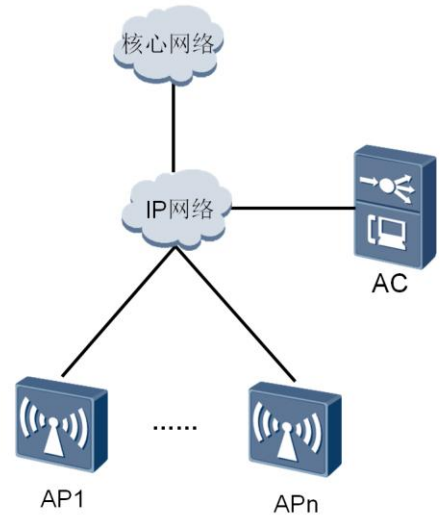


 Page8 HUAWEI

- 直连式组网可以认为AP、AC与上层网络串联在一起，所有数据必须通过AC到达上层网络。
- 采用这种组网方式，对AC的吞吐量以及处理数据能力比较高，否则AC会是整个无线网络带宽的瓶颈。但用此种组网，组网架构清晰，组网实施起来简单。

瘦AP+AC组网方式（续）

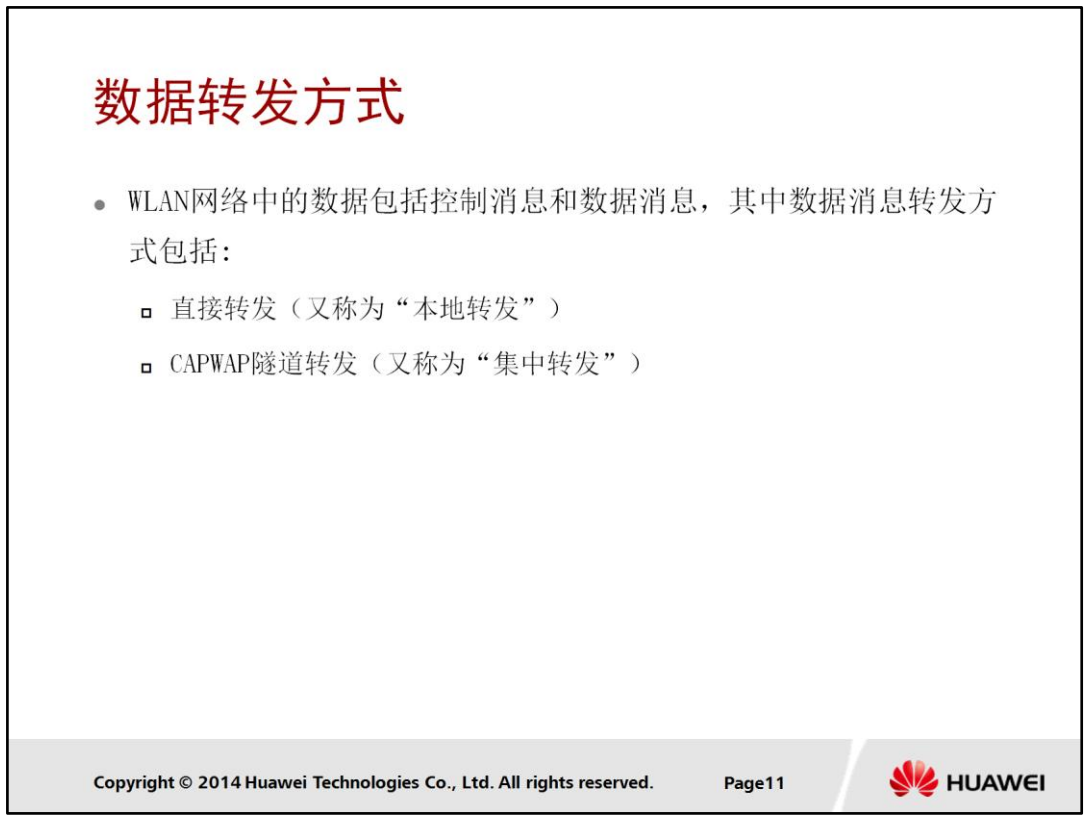
- 旁挂式组网
  - 旁挂式组网，AC旁挂在AP与上行网络的直连网络上，AP的业务数据可以不经AC而直接到达上行网络。



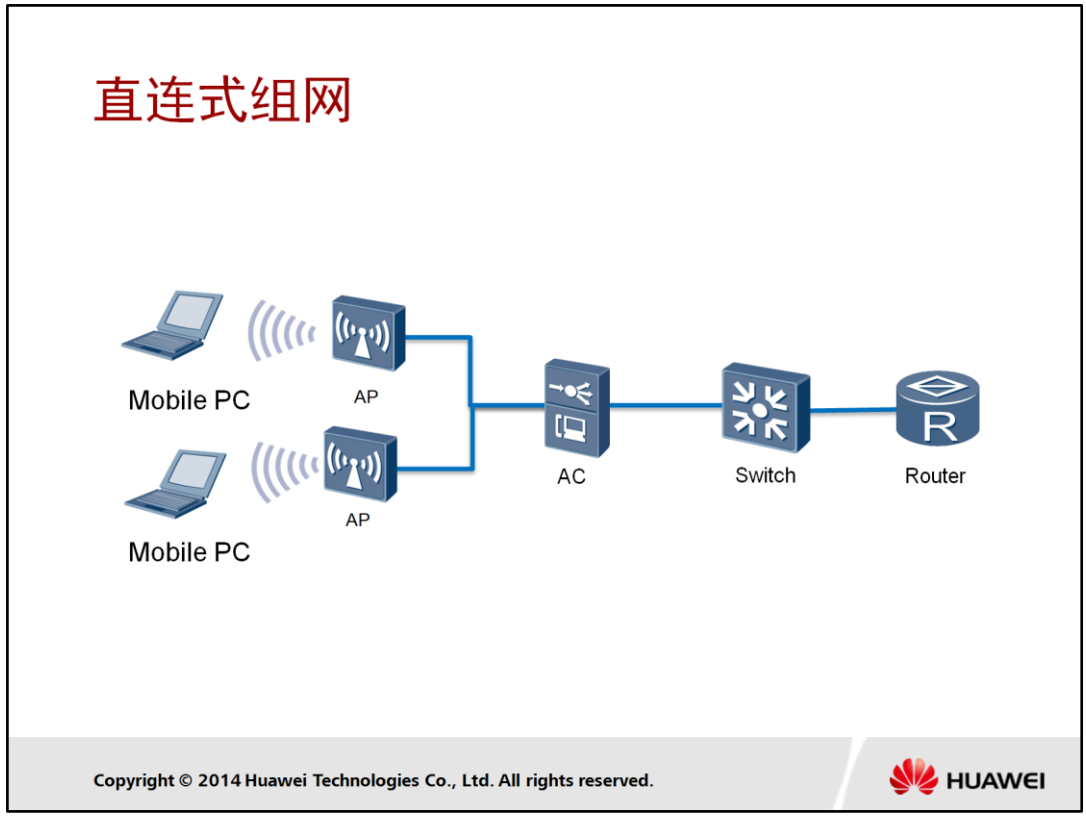
  HUAWEI

- 旁挂式组网，AC旁挂在AP与上行网络的直连网络中，不再直接连接AP。
- 由于实际组网中，大部分不是早期就规划好无线网络，无线网络的覆盖架设大部分是后期在现有网络中扩展而来。而采用旁挂式组网就比较容易进行扩展，只需将AC旁挂在现有网络中，比如旁挂在汇聚交换机上，就可以对终端AP进行管理。所以此种组网方式使用率比较高。
- 在旁挂式组网中，AC只承载对AP的管理功能，管理流封装在CAPWAP隧道中传输。数据业务流可以通过CAPWAP数据隧道经AC转发，也可以不经过AC转发直接转发，后者无线用户业务流经汇聚交换机由汇聚交换机传输至上层网络。

目 录

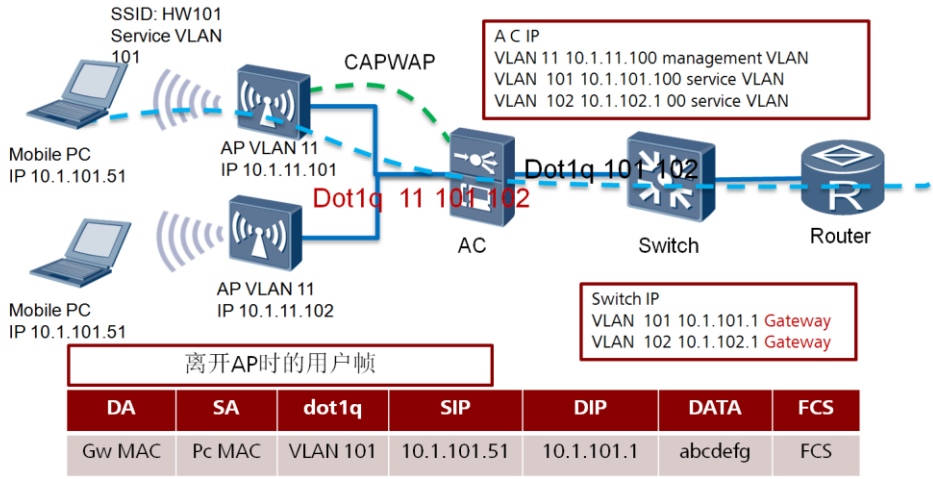


- AC6605承载管理流和数据业务流，管理流必须封装在CAPWAP（Control And Provisioning of Wireless Access Points）隧道传输，数据流可以根据实际情况选择是否封装在CAPWAP隧道中传输。
- CAPWAP定义了无线接入点（AP）与无线控制器（AC）之间的通信规则，为实现AP和AC之间的互通性提供通用封装和传输机制。
  - CAPWAP数据隧道封装发往AC6605的802.11协议的数据包。
  - CAPWAP管理隧道提供远程AP配置和WLAN管理。
- 根据数据流（也称业务流）是否封装在CAPWAP隧道中转发，可以分为两种转发模式：
  - 直接转发：也称本地转发或分布转发。
  - 隧道转发：也称集中转发，通常用于集中控制无线用户流量的场景。
- 无论直连式组网还是旁挂式组网，都可以根据需要自行选择，AC6605支持两种模式混合，即根据需要部分AP配置为直接转发模式，部分AP配置为隧道转发模式。由于隧道转发模式下，所有无线用户流量都将汇聚到AC上处理，存在交换瓶颈的风险，在企业网中不常采用。



- 直连式组网是指AC6605下直接接入AP或接入交换机，同时扮演AC和汇聚交换机功能，AP的数据业务和管理业务都由AC6605集中转发和处理。
- 直连式组网方式中，AP和AC6605之间建立CAPWAP管理隧道，AC通过该CAPWAP管理隧道实现对AP的集中配置和管理。无线用户的业务数据可以通过CAPWAP数据隧道在AP与AC之间转发（隧道转发模式），也可以由AP直接转发（直接转发模式）。
- 由于直连式组网中，AC自然串接在线路中，故多采用直接转发模式，用户业务数据在AP上实现转发。
- AC6605启动DHCP Server功能，给AP分配IP地址，AP通过DNS或DHCP option43的方式或二层发现协议发现AC6605，建立数据业务通道。

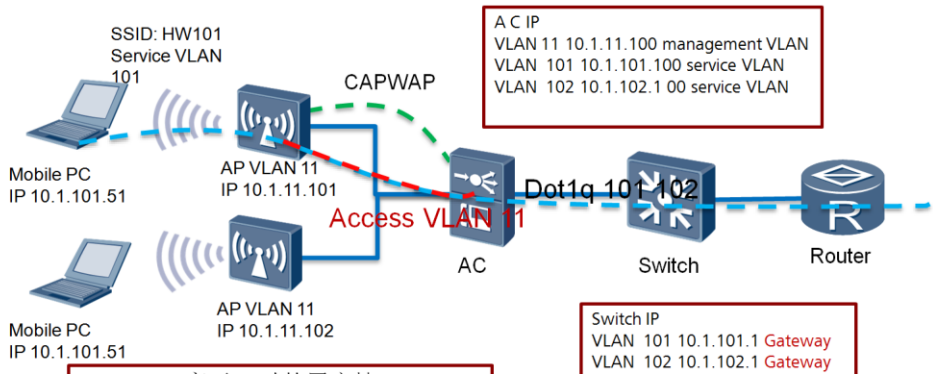
直连式组网-直接转发



离开AP时的用户帧

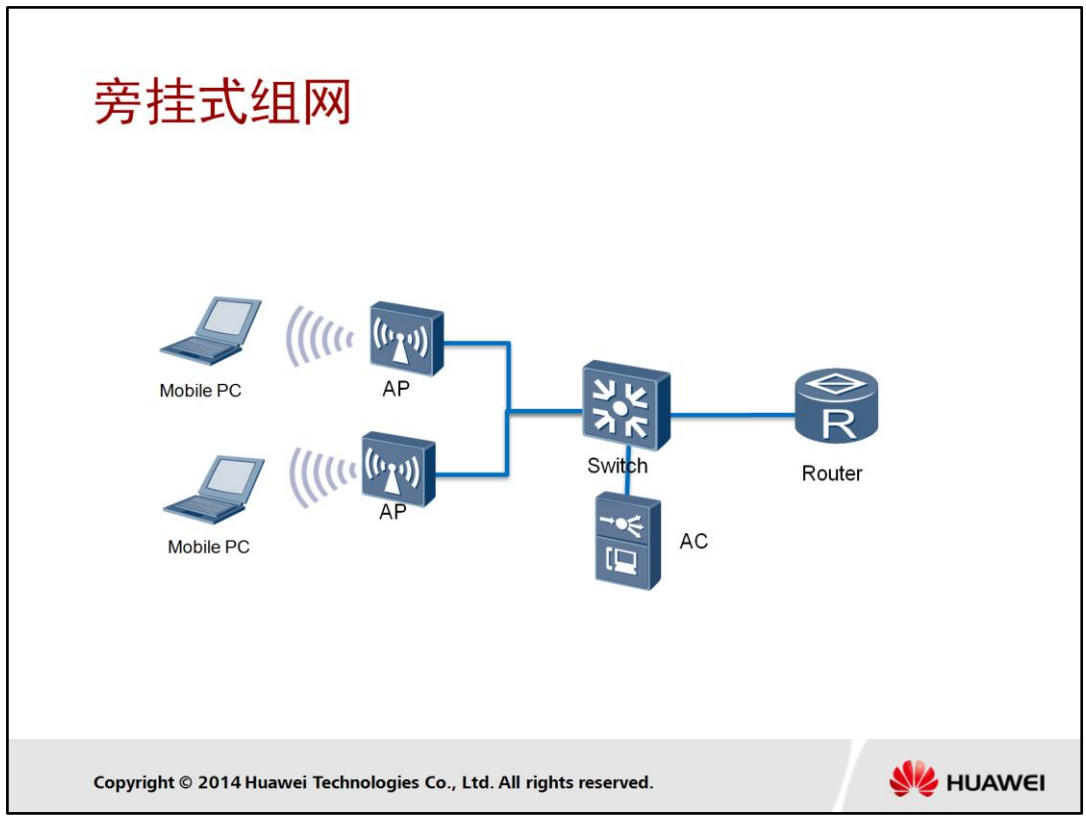
DA	SA	dot1q	SIP	DIP	DATA	FCS
Gw MAC	Pc MAC	VLAN 101	10.1.101.51	10.1.101.1	abcdefg	FCS

直连式组网-隧道转发



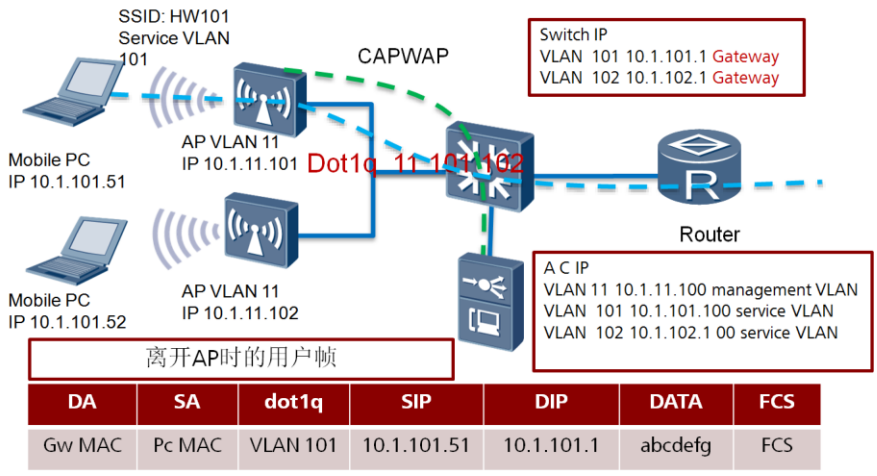
离开AP时的用户帧

DA	SA	dot1q	SIP	DIP	DATA	FCS
AC MAC	AP MAC	NULL	10.1.11.101	10.1.11.100	CAPWAP user data	FCS



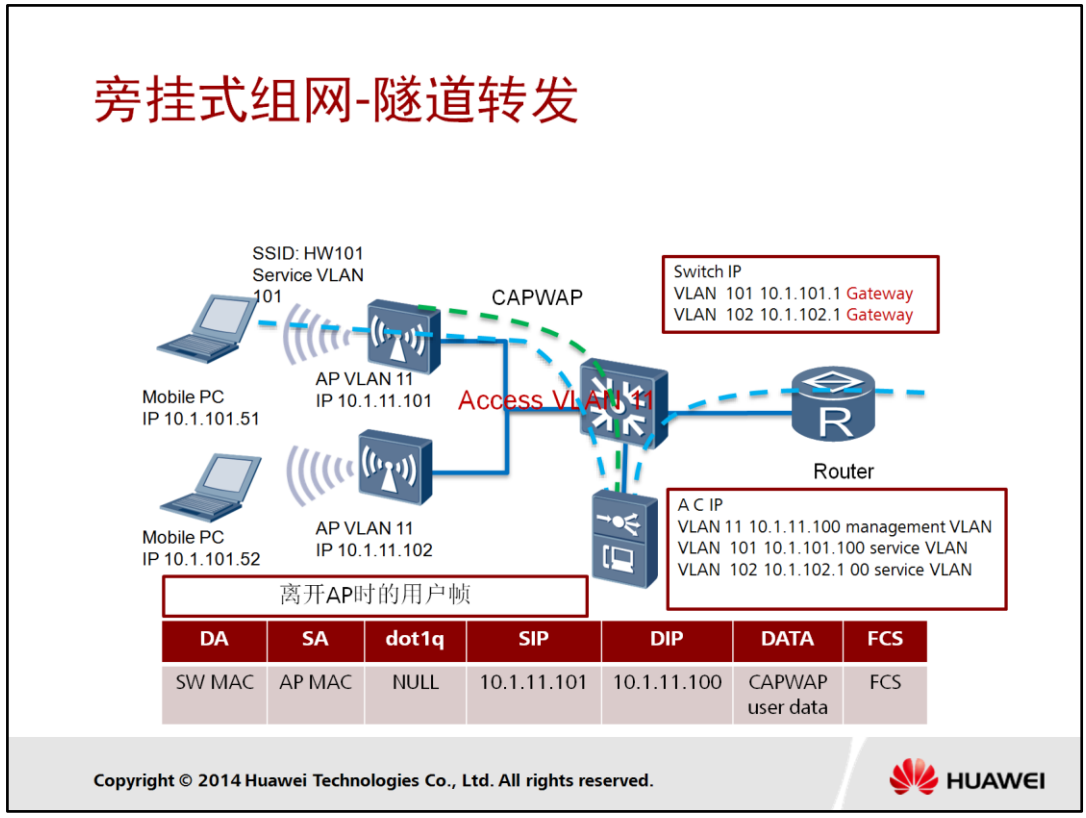
- 旁挂式组网是指AC6605旁挂在现有网络中（多在汇聚交换机旁边），实现对AP的WLAN业务管理。
- 在旁挂式组网中，AC6605只承载对AP的管理功能，管理流封装在CAPWAP隧道中传输。数据业务流可以通过CAPWAP数据隧道经AC转发，也可以不经过AC转发直接转发，后者无线用户业务流经汇聚交换机传输至上层网络。

旁挂式组网-直接转发



DA	SA	dot1q	SIP	DIP	DATA	FCS
Gw MAC	Pc MAC	VLAN 101	10.1.101.51	10.1.101.1	abcdefg	FCS

- 直接转发又称为数据本地转发，即AP与AC间的报文没有经过CAPWAP隧道封装，直接转发到上层网络，从而提高报文的转发效率。
- 直接转发指AP不会对数据报文进行任何处理，发送原始报文。
- 采用直接转发，可以很容易的突破AC的带宽限制，而且配置CAPWAP断链保持以后，可以减少无线用户断网的风险。

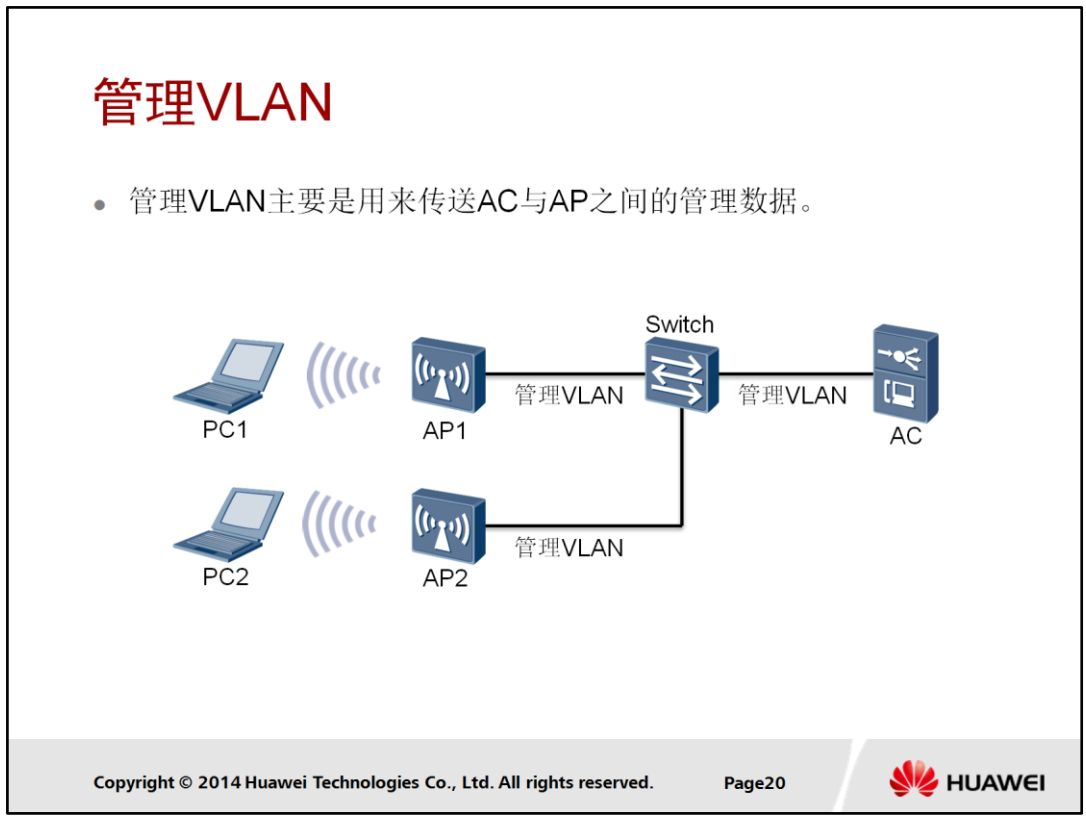


- 隧道转发又称为集中转发，即AP与AC间的报文经过CAPWAP隧道封装后再转发到上层网络，从而提高报文的转发安全性。
- 隧道转发，所有数据报文都要经过CAPWAP隧道封装后到达AC，再由AC转发到上层网络。
- 采用此种数据转发方式，可以大大提高数据的安全性，还可以对数据进行集中控制，比如QoS等。

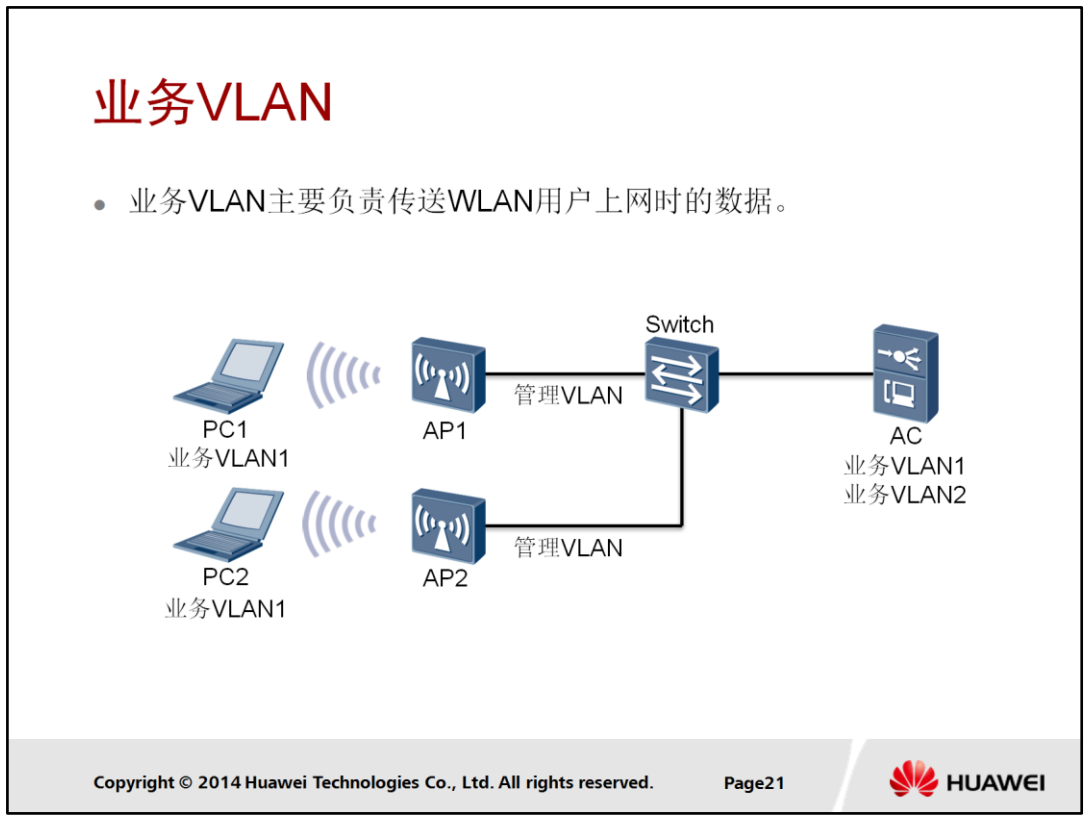
数据转发方式

- AP与AC间的控制报文必须采用CAPWAP隧道进行转发，而数据报文则除了可以采用CAPWAP隧道转发之外，还可以采用直接转发方式。
- 当AC为旁挂式组网（即AC的业务接入端口和上行端口为同一个以太网端口）时，如果数据是直接转发，则数据流不经过AC；如果数据是隧道转发模式，则数据流经过AC。

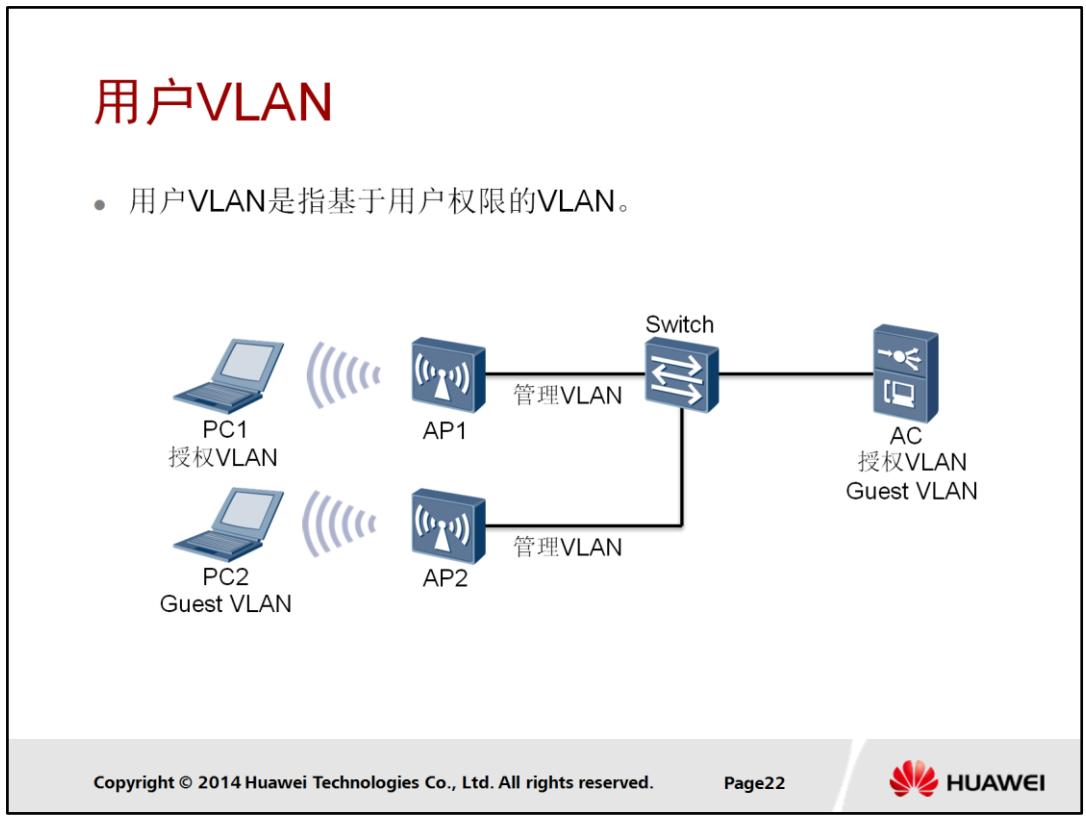
目 录



- 管理VLAN：
  - 对于二层交换机而言，一般只能设置一个三层虚接口，所以必须设置一个VLAN作为三层虚接口的管理VLAN。管理VLAN中绑定了一个IP地址，这样我们可以远程管理交换机，例如登录交换机查看相应的LOG日志，分析交换机状态，处理某些故障等。
  - 对于WLAN来说，管理VLAN主要是用来传送AC与AP之间的管理数据，如AP DHCP报文、AP ARP报文、AP CAPWAP报文（包含控制CAPWAP报文和数据CAPWAP报文）。AC内部XGE口的PVID和TRUNK VLAN与交换机普通物理端口的PVID和TRUNK VLAN相同，在部署AC时，需要配置PVID为管理VLAN ID并允许管理VLAN的报文通过TRUNK接口。

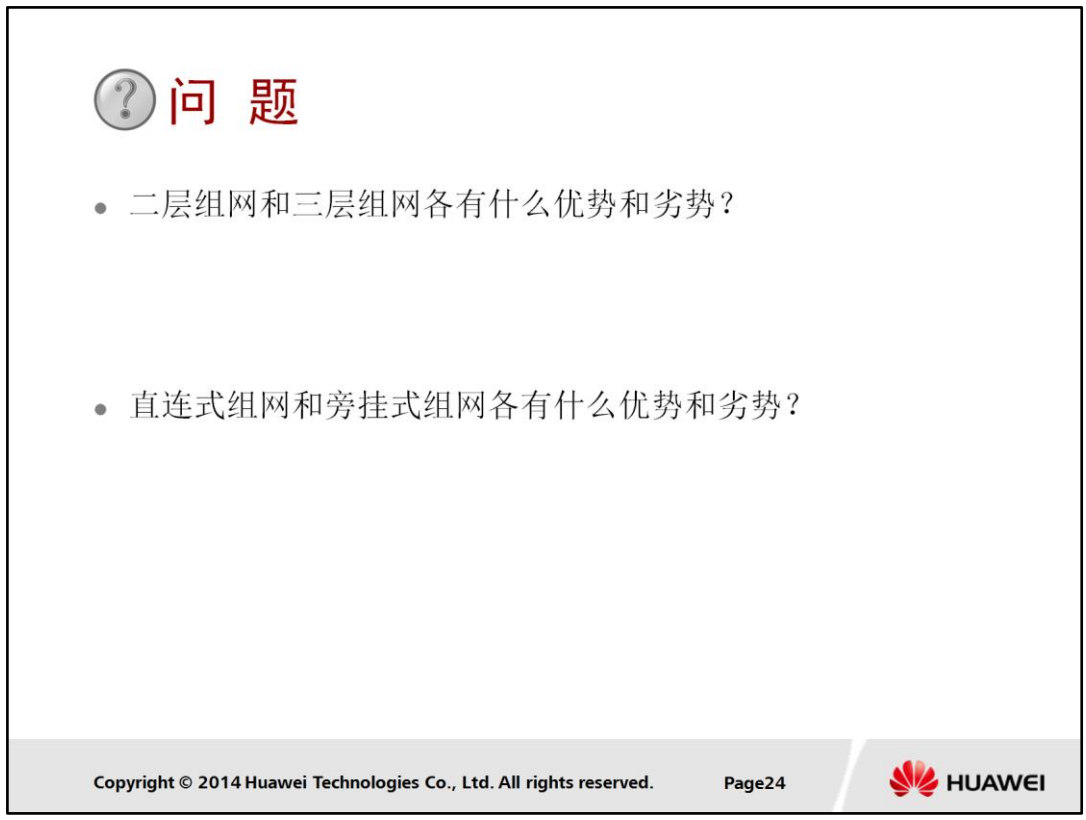


- 从WLAN整体来看：
  - 业务VLAN是基于VAP的区域业务VLAN，与位置有关，与用户无关，VAP内的用户使用此业务VLAN封装用户。主要负责传送WLAN用户上网时的数据。
- 从AP角度看：
  - 直接转发模式下，业务VLAN是指AP给数据报文加的VLAN。
  - 隧道转发模式下，业务VLAN是指CAPWAP隧道内用户报文的VLAN。
- 从AC角度看：
  - WLAN ESS接口的PVID VLAN：管理员手工配置，仅在AP发送的用户报文为Untag时生效，表示的是AC发送和接收的用户报文的缺省VLAN。
  - 服务集模板中的Service VLAN：AP上传的用户报文VLAN，始终为当前用户的业务VLAN。



- 用户VLAN是指基于用户权限的VLAN，WLAN中使用的用户VLAN具体可以分为以下几种：
- 用户在使用802.1X方式进行用户接入安全认证时，会涉及到以下的VLAN：
  - Guest VLAN：
    - Guest VLAN的基本功能是使用户在没有经过认证的情况下也能访问Guest VLAN内部的部分资源。例如，当用户没有安装客户端软件时，可以通过访问Guest VLAN的资源下载并安装客户端，通过认证后，才能进行正常的网络访问。
  - Restrict VLAN：
    - Restrict VLAN功能允许用户在认证失败的情况下可以访问某一特定VLAN中的资源，这个VLAN称之为Restrict VLAN。需要注意的是，这里的认证失败是认证服务器因某种原因明确拒绝用户认证通过，比如用户密码错误，而不是认证超时或网络连接等原因造成的认证失败（即AC收到RADIUS服务器下发的Radius-reject报文）。
- 授权VLAN：
  - 传统的静态VLAN部署不仅管理复杂，而且难以解决移动办公用户的VLAN控制问题。可以通过在用户接入网络时动态指定该用户所属的VLAN，实现基于用户的VLAN划分。例如，在企业网中，通过动态VLAN下发，可以保证在无线用户在一个AP的覆盖区域漫游到另外一个AP的覆盖区域时，用户均属于同一个业务VLAN，保证用户正常业务不被中断。

- VLAN部署的原则
- 当WLAN系统同时设置了用户VLAN和管理、业务VLAN后，原则如下：
  - 无论在认证、重认证、漫游重认证还是CoA动态下发VLAN过程中，授权VLAN都有最高优先级，且为即时启用。
  - 如果认证、重认证、漫游重认证还是CoA动态下发VLAN过程中没有授权VLAN，则取用当前所在地的业务VLAN。
  - 总体而言，用户VLAN优先于业务VLAN，在系统同时设置有授权VLAN、Guest VLAN、Restrict VLAN等用户VLAN的情况下，优先启用授权VLAN。



- 二层组网和三层组网各有什么优势和劣势？
  - 二层组网的优势
    - 二层组网组网简单，配置容易，适用于简单临时的组网，能够进行比较快速的组网配置。
  - 三层组网的优势
    - 在实际组网中，一台AC可以连接几十甚至几百台AP，组网一般比较复杂。比如在企业网络中，AP可以布放在办公室，会议室，会客间等场所，而AC可以安放在公司机房，这样，AP和AC之间的网络就是比较复杂的三层网络。因此，在大型组网中一般采用三层组网。
- 直连式组网和旁挂式组网各有什么优势和劣势？
  - 直连式组网优势
    - 在直连式组网中，多采用直接转发模式，适用于大规模集中部署的WLAN网络，并可以简化网络架构。
  - 旁挂式组网优势
    - 这种方式是常用的组网模式，此时无线用户业务数据无需经过AC集中处理，基本无带宽瓶颈，而且便于继承现有网络的安全策略，故此模式也多是推荐的网络部署方案。

总 结

- WLAN组网方式
- WLAN数据转发方式

谢谢

www.huawei.com