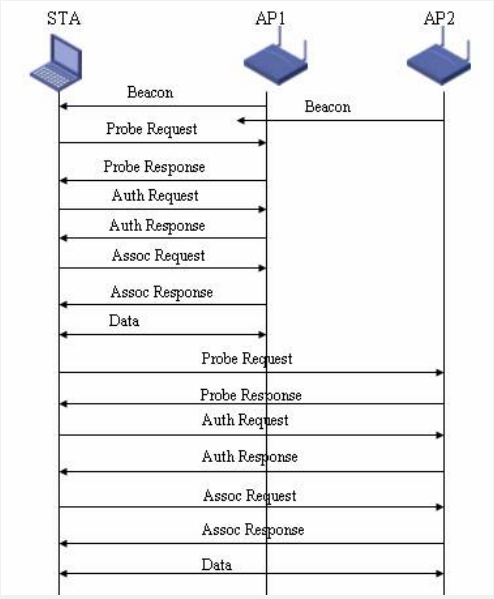
无线(WLAN)技术漫游实现描述

宋斌 2008-09-09 发表

【运营商】

无线(WLAN)技术漫游实现描述

一、FAT AP架构下，AP设备不做认证时：



(1) AP1，AP2正常工作，发送Beacon帧，向STA通告支持的无线服务；

(2) STA搜索到AP1的信号，向AP1发Probe Request,请求获取AP1所提供的无线服务；AP1回应Probe Response；

(3) STA向AP1发送认证请求报文（Authentication Request）请求接入，AP1回应认证响应报文(Authentication Response);

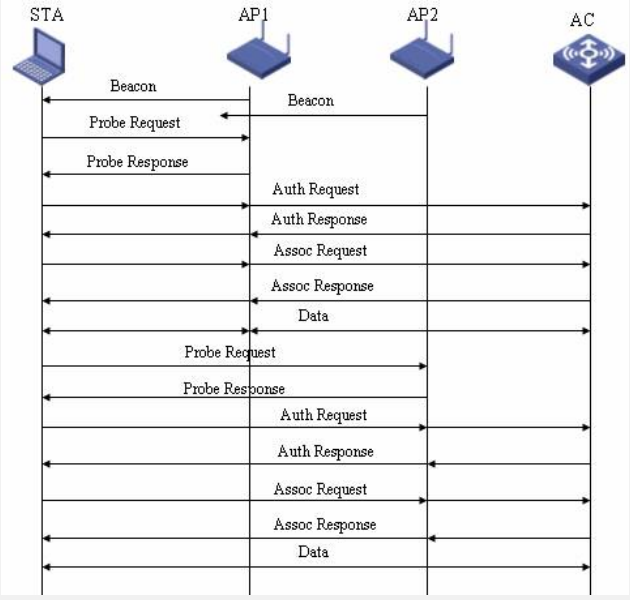
(4) STA向AP1发送关联请求报文（Association Request）进行关联，AP1回应关联响应报文(Association Response)。STA与AP间建立链路层连接;

(5) STA不需要进行身份认证，通过AP1成功连入网络。

(6) 当STA从AP1往AP2方向移动，感知到AP2的信号强度渐大，AP1强度渐弱，当AP2与AP1的信号强度差达到一定门限时，STA开始向AP2发起认证和关联请求，（通过Probe Request/Response, Authentication Request/Response以及Association Request/Response报文）；

(7) STA与AP2的链路层连接建立成功后，成功连入网络。

二、AC+FIT AP架构下，AC上不做认证时：

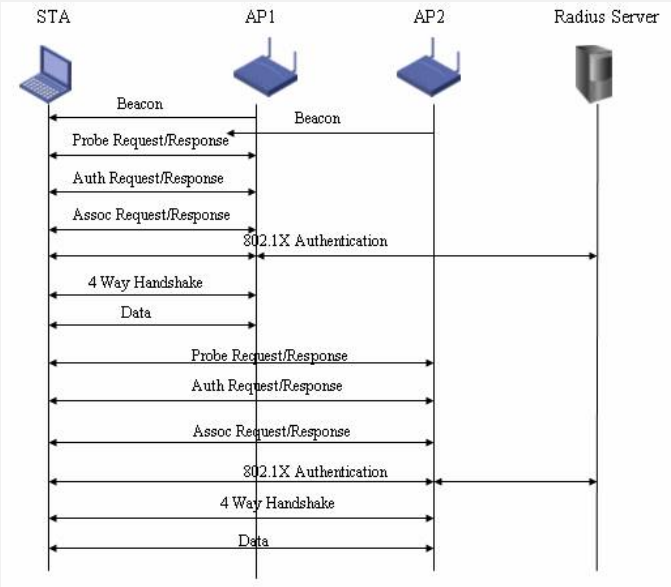


(1) AP1与AP2分别与AC建立CAPWAP隧道；

(2) AP1，AP2发送Beacon帧，向STA通告支持的无线服务；

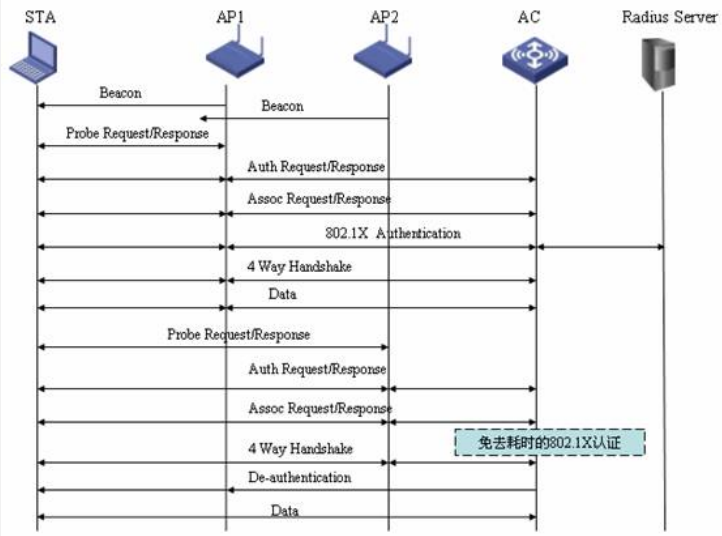
(3) STA搜索到AP1的信号，向AP1发Probe Request,请求获取AP1所提供的无线服务；AP1回应Probe Response;
(4) STA向AP1发送认证请求报文（Authentication Request）请求接入，AP1透传报文到AC，AC通过AP1回应认证响应报文(Authentication Response);
(5) STA向AP1发送关联请求报文（Association Request）进行关联，AP1透传报文至AC，AC回应关联响应报文(Association Response)。STA与AP1间建立链路层连接;
(6) STA不需要进行身份认证，通过AP1成功连入网络。
(7) 当STA从AP1往AP2方向移动，感知到AP2的信号强度渐大，AP1强度渐弱，当AP2与AP1的信号强度差达到一定门限时，STA开始向AP2发起认证和关联请求，（通过Probe Request/Response, Authentication Request/Response以及Association Request/Response报文），建立无线链路连接;
(8) AC通过AP1向STA发送一个去认证报文，通知STA从AP1下线;
(9) STA通过AP2成功连入网络。

三、FAT AP架构下，在AP上进行802.1X认证时:



(1) AP1，AP2正常工作，发送Beacon帧，向STA通告支持的无线服务;
(2) STA搜索到AP1的信号，向AP1发Probe Request,请求获取AP1所提供的无线服务；AP1回应Probe Response;
(3) STA向AP1发送认证请求报文（Authentication Request）请求接入，AP1回应认证响应报文(Authentication Response);
(4) STA向AP1发送关联请求报文（Association Request）进行关联，AP1回应关联响应报文(Association Response)。STA与AP间建立链路层连接;
(5) AP1向STA发起802.1X协商，用户输入用户名、密码，AP1通过Radius协议把用户名、密码发到Radius服务器上进行认证。
(6) 802.1X认证成功后，STA与服务器间协商出PMK，同时服务器把PMK下发到AP1上。
(7) STA与AP1进行四次握手协商，通过PMK协商得到STA与AP1间数据加密所用的PTK。
(8) STA通过AP1成功连入网络。
(9) 当STA从AP1往AP2方向移动，感知到AP2的信号强度渐大，AP1强度渐弱，当AP2与AP1的信号强度差达到一定门限时，STA开始向AP2发起认证和关联请求，（通过Probe Request/Response, Authentication Request/Response以及Association Request/Response报文）;
(10) STA与AP2的链路层连接建立成功后，因AP2上没有STA的身份信息，因此还需要与STA进行802.1X协商，并得到STA与AP2之间的PMK;
(11) 802.1X协商成功后，STA与AP2进一步通过四次握手协商数据加密密钥PTK;
(12) STA通过AP2成功连入网络。

四、AC+FIT AP架构下，AC上做802.1X认证时:



(1) AP1与AP2分别与AC建立CAPWAP隧道；
(2) AP1，AP2发送Beacon帧，向STA通告支持的无线服务；
(3) STA搜索到AP1的信号，向AP1发Probe Request,请求获取AP1所提供的无线服务；AP1回应Probe Response；
(4) STA向AP1发送认证请求报文（Authentication Request）请求接入，AP1透传报文到AC，AC通过AP1回应认证响应报文(Authentication Response)；
(5) STA向AP1发送关联请求报文（Association Request）进行关联，AP1透传报文至AC，AC回应关联响应报文(Association Response)。STA与AP1间建立链路层连接；
(6) AP1与STA开始802.1X协商，用户输入用户名、密码，AC通过Radius协议把用户名、密码发到Radius服务器上进行认证。
(7) 802.1X认证成功后，STA与服务器间协商出PMK，同时服务器把PMK下发到AC上。
(8) STA与AC之间进行四次握手协商，通过PMK协商得到STA与AP1间数据加密所用的PTK，AC把PTK下发到AP1上。
(9) STA通过AP1成功连入网络。
(10) 当STA从AP1往AP2方向移动，感知到AP2的信号强度渐大，AP1强度渐弱，当AP2与AP1的信号强度差达到一定门限时，STA开始向AP2发起认证和关联请求，（通过Probe Request/Response, Authentication Request/Response以及Association Request/Response报文）；
(11) STA与AP2的链路层连接建立成功后，因AC上已经有STA的身份信息，因此不需要再进行802.1X协商，而是直接使用之前得到的PMK进行STA与AP2间的四次握手协议协商AP2与STA间的数据加密密钥PTK；
(12) AC通过AP1向STA发送一个去认证报文，通知STA从AP1下线；
(13) STA通过AP2成功连入网络。