



802.11 PMK的生成方式

wlan安全

朱恺

2017-12-27 发表

802.11协议规范了PMK (Pairwise Master Key) 长度必须为256bits, 即32字节。在WPA-PSK/WPA2-PSK模式下, PMK是人为手动输入配置的。但是在802.1X认证环境下, PMK是通过Radius Server与AC或者AP计算出来, 通过Radius Access-accept的MS-MPPE-Vendor-Specific属性字段携带, 该属性字段一般为MD5加密, 通过前期Radius交互之后, MD5解密出明文的32字节PMK。