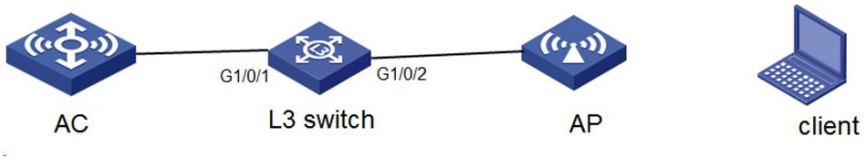
V7 AC与AP间capwap隧道加密功能实现

AP管理 刘小虎 2017-02-08 发表

目前V7版本中的FIT AP与AC之间通过capwap隧道来通信，但此时的数据并未经过加密通过wireshark等抓包软件可以直接抓取、解读数据。而随着大家对数据安全越来越重视，对AC与AP间隧道数据的加密也就显得非常有必要了，目前V7版本中可以通过简单的配置就实现AP与AC间capwap隧道的加密。



组网说明：AC与AP交换机相连，AP通过二层或三层注册方式均可，此案例中已二层注册方式为例。AP管理vlan为VLAN 100，dhcp server位于AC上。

配置步骤：

1、AC侧配置

```
#
wlan ap ap1 model WA4320-ACN-SI
 serial-id 219801A0T78166E00061
tunnel encryption enable //在AC与AP侧导入相应文件后，开启AP与AC间的隧道加密功能
 radio 1
  radio 2
#
interface Vlan-interface100
 ip address 192.168.100.254 255.255.255.0
#
dhcp server ip-pool vlan100
 gateway-list 192.168.100.254
 network 192.168.100.0 mask 255.255.255.0
#
```

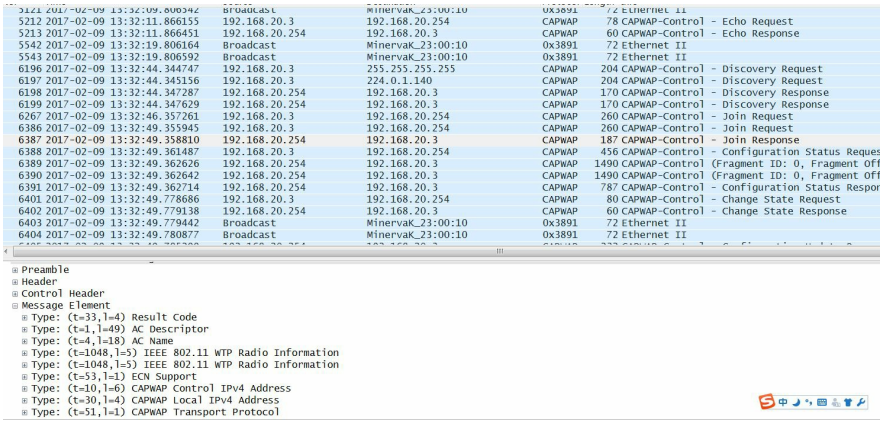
2、SW侧配置

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
poe enable
#
```

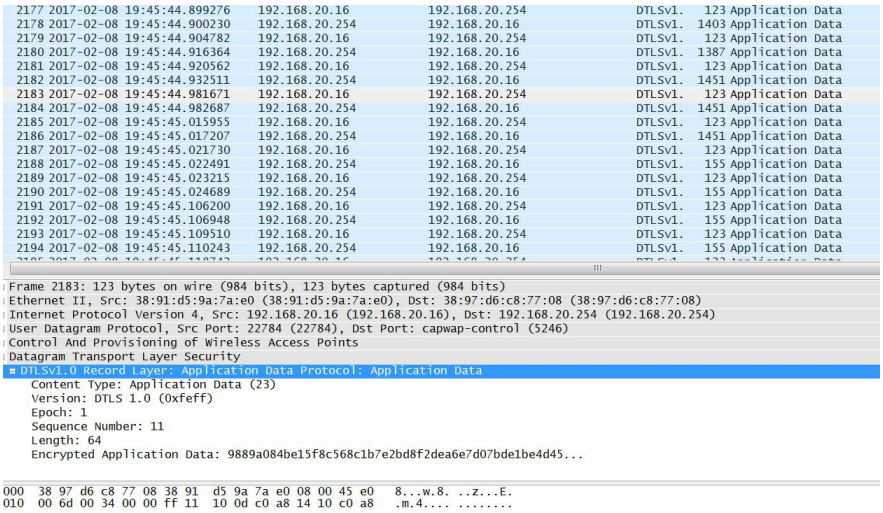
结果验证：

从抓包来看加密后AC与AP间交互报文已被加密。

1、加密前AC与AP间报文交互



2、加密后AC与AP间报文交互



1、一定要将相应的*.pem文件分别导入到AC与AP的根目录下。在AC的根目录下导入root.pem、server.pem文件；在AP根目录下导入root.pem、client.pem文件 //*.pem文件不区分AC与AP具体型号。

2、AP需在AC上线后再执行隧道加密配置，证书文件导入操作及加密配置完成后需让AP重新执行一次上线流程。