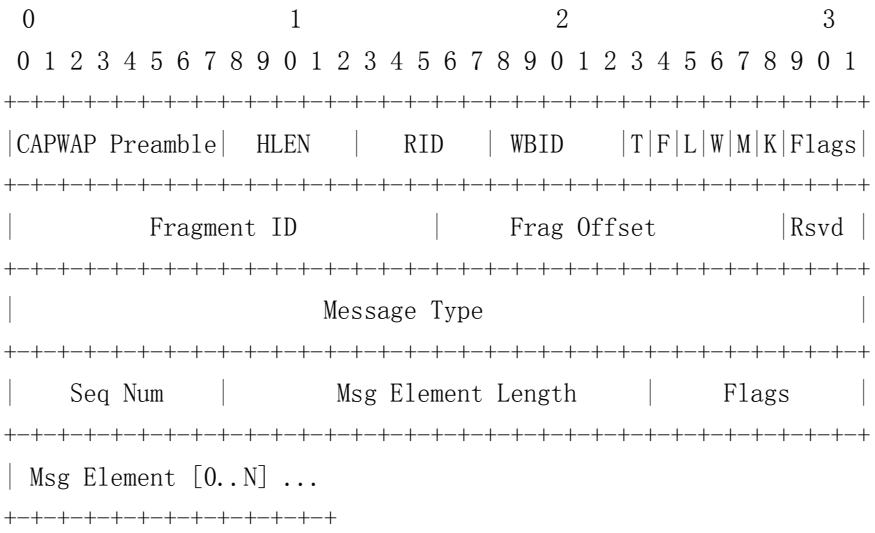
CAPWAP 报文分析

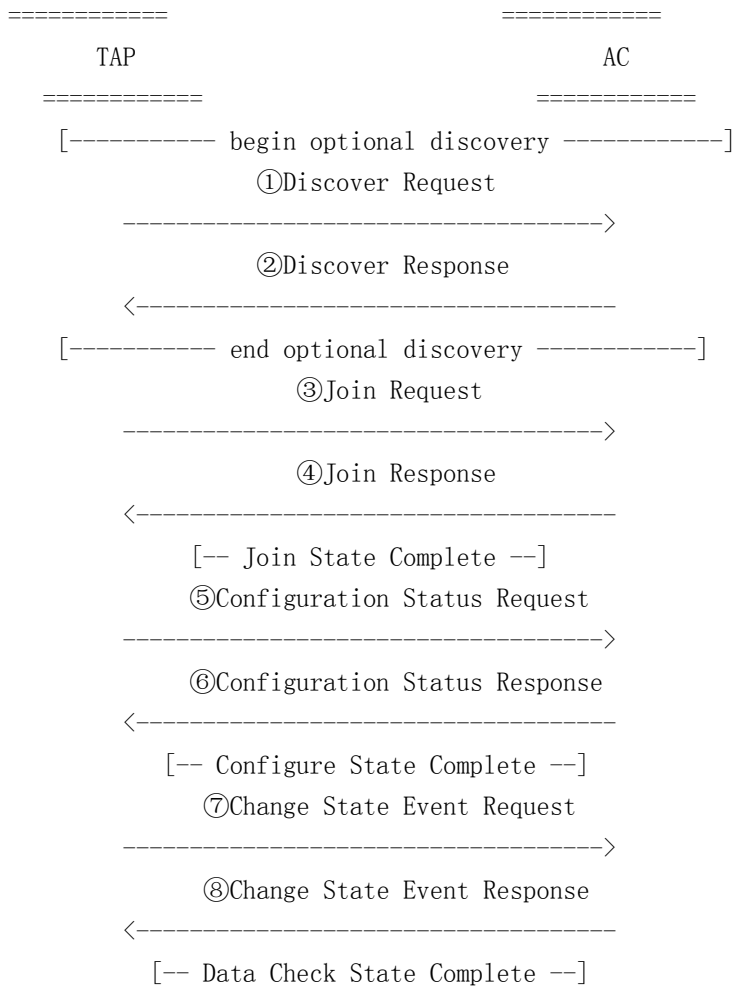
Member	Role	E-mail	Department
zhuxiaoyan	Engineer	aimee@zcom.nj	RD2(2010-6-2)

一、 CAPWAP 报文

1、CAPWAP 报文格式



2、AC 和 AP 的报文交互过程



(-- enter RUN state --)

:

:

Echo Request

---------->

Echo Response

<----------

:

:

Event Request

---------->

Event Response

<----------

3、CAPWAP 报文类型（CAPWAP Message Type）值的对应表

CAPWAP Control Message	Message Type Value
Discovery Request	1
Discovery Response	2
Join Request	3
Join Response	4
Configuration Status Request	5
Configuration Status Response	6
Configuration Update Request	7
Configuration Update Response	8
WTP Event Request	9
WTP Event Response	10
Change State Event Request	11
Change State Event Response	12
Echo Request	13
Echo Response	14
Image Data Request	15
Image Data Response	16
Reset Request	17
Reset Response	18
Primary Discovery Request	19
Primary Discovery Response	20
Data Transfer Request	21
Data Transfer Response	22
Clear Configuration Request	23
Clear Configuration Response	24
Station Configuration Request	25
Station Configuration Response	26

4、CAPWAP 报文中 Message Type 的计算方法

Message Type =IANA Enterprise Number * 256 +
Enterprise Specific Message Type Number

IANA Enterprise Number：IANA 的企业数（这个由制定者定义的值），ZDC 定义此值为 13277，13277*256=3398912，转换成十六进制位 00 33 DD 00，Enterprise Specific Message Type Number 真正的 Message Type value。

二、 CAPWAP 报文分析

1、 抓包方法

使用 HUB 抓 5246 端口号的报文。

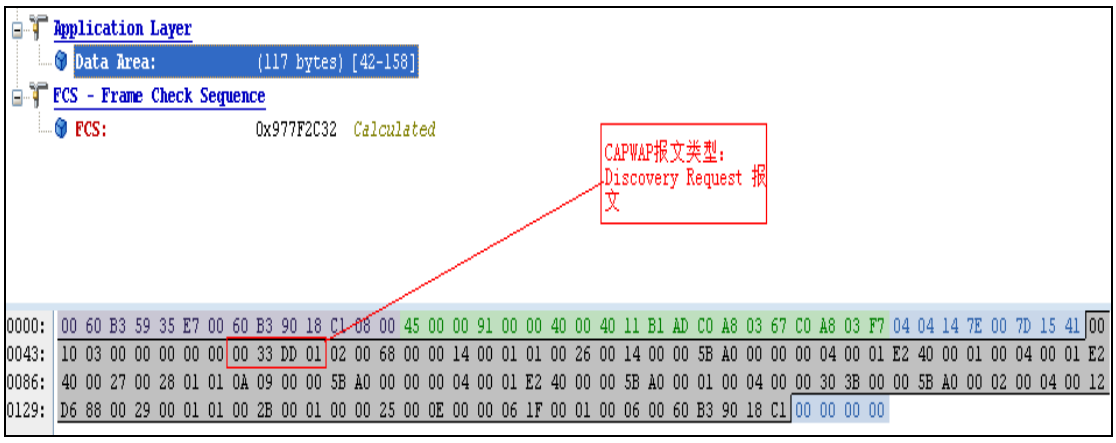
2、 抓包截图

1	IP-192.168.3.103	IP-1028	IP-192.168.3.247	IP-5246	163	0.000000	UDP
2	IP-192.168.3.247	IP-5246	IP-192.168.3.103	IP-1028	121	0.000336	UDP
3	IP-192.168.3.103	IP-1028	IP-192.168.3.247	IP-5246	192	0.001125	UDP
4	IP-192.168.3.247	IP-5246	IP-192.168.3.103	IP-1028	129	0.005400	UDP
5	IP-192.168.3.103	IP-1028	IP-192.168.3.247	IP-5246	132	0.006026	UDP
6	IP-192.168.3.247	IP-5246	IP-192.168.3.103	IP-1028	129	0.006435	UDP
7	IP-192.168.3.103	IP-1028	IP-192.168.3.247	IP-5246	77	0.006902	UDP
8	IP-192.168.3.247	IP-5246	IP-192.168.3.103	IP-1028	64	0.007235	UDP
9	IP-192.168.3.247	IP-5246	IP-192.168.3.103	IP-1028	1518	0.008582	UDP
10	IP-192.168.3.247	IP-5246	IP-192.168.3.103	IP-1028	1518	0.009915	UDP
11	IP-192.168.3.247	IP-5246	IP-192.168.3.103	IP-1028	343	0.010246	UDP
12	IP-192.168.3.103	IP-1028	IP-192.168.3.247	IP-5246	1518	0.187184	UDP
13	IP-192.168.3.103	IP-1028	IP-192.168.3.247	IP-5246	1518	0.188512	UDP
14	IP-192.168.3.103	IP-1028	IP-192.168.3.247	IP-5246	1518	0.189511	UDP
15	IP-192.168.3.103	IP-1028	IP-192.168.3.247	IP-5246	978	0.190513	UDP
16	IP-192.168.3.247	IP-5246	IP-192.168.3.103	IP-1028	64	0.190845	UDP
17	IP-192.168.3.103	IP-1028	IP-192.168.3.247	IP-5246	318	1.615581	UDP
18	IP-192.168.3.103	IP-1028	IP-192.168.3.247	IP-5246	272	1.618976	UDP
19	IP-192.168.3.247	IP-5246	IP-192.168.3.103	IP-1028	64	1.619518	UDP
20	IP-192.168.3.103	IP-1028	IP-192.168.3.247	IP-5246	272	5.581168	UDP
21	IP-192.168.3.247	IP-5246	IP-192.168.3.103	IP-1028	64	5.581517	UDP
22	IP-192.168.3.103	IP-1028	IP-192.168.3.247	IP-5246	272	5.585034	UDP
23	IP-192.168.3.247	IP-5246	IP-192.168.3.103	IP-1028	64	5.585367	UDP
24	IP-192.168.3.103	IP-1028	IP-192.168.3.247	IP-5246	64	9.831798	UDP
25	IP-192.168.3.247	IP-5246	IP-192.168.3.103	IP-1028	64	9.832126	UDP

3、 分析报文

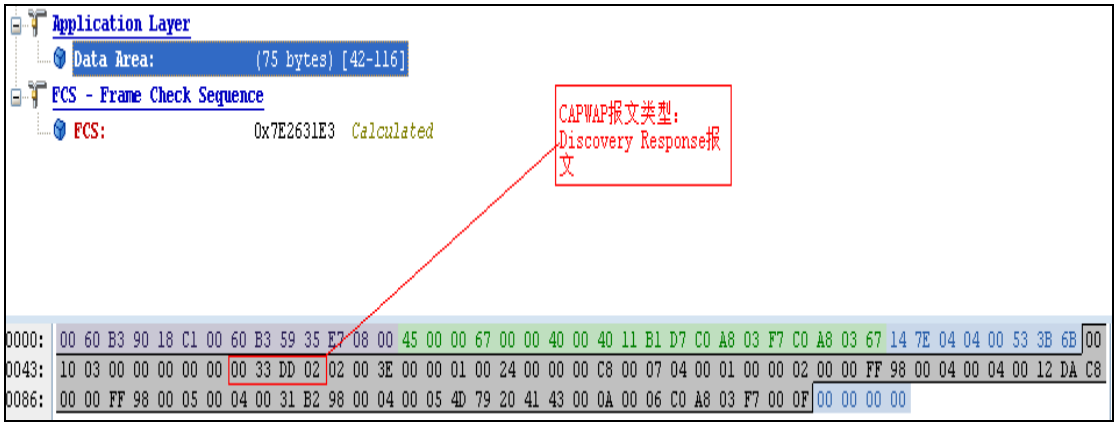
打开报文主要看 Data Area 部分进行分析，

(1)第一个报文截图如下：



点到 Data Area 之后，可以选中它的内容部分，图中黑色区域 00 10 03 00 00 00 00 00 代表 CAPWAP 协议头(注：前八个字节代表 CAPWAP 协议头)。之后的四个字节就是 CAPWAP 的报文类型，即 CAPWAP Control Message type value。如第一个包为 00 33 DD 01，那么按照先前介绍的计算方法，00 33 DD 00 为 IANA 的企业数，所以 01 是真正的 CAPWAP Control Message type value，由 CAPWAP 报文类型(CAPWAP Message Type)值的对应表可以看到，第一个报文为 Discovery Request 报文。

(2) 第二个报文截图如下：



点到 Data Area 之后，可以选中它的内容部分，图中黑色区域 00 10 03 00 00 00 00 00 代表 CAPWAP 协议头(注：前八个字节代表 CAPWAP 协议头)。之后的四个字节就是 CAPWAP 的报文类型，即 CAPWAP Control Message type value。如第一个包为 00 33 DD 02，那么按照先前介绍的计算方法，00 33 DD 00 为 IANA 的企业数，所以 02 是真正的 CAPWAP Control Message type value，由 CAPWAP 报文类型(CAPWAP Message Type)值的对应表可以看到，第一个报文为 Discovery Request 报文。

同样依次分析 3，4，5，6，7，8 报文为 Join Request 报文，Join Response 报文，Configuration Status Request 报文，Configuration Status Response 报文，Change State Event Request 报文，Change State Event Response 报文，之后的报文就是进入运行状态后的报文（enter RUN state）。