

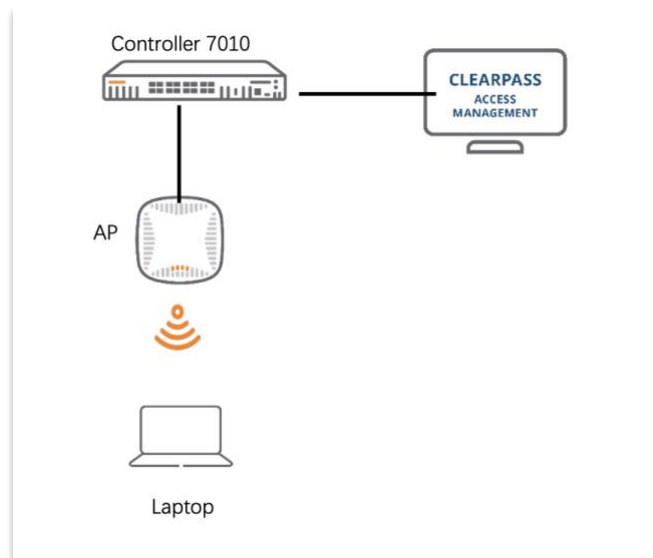
ARUBA 控制器对接
外部 Portal Server
-User post credential 流程

yangh@xinyuming.com.cn

lifz@cvanguard.com

2026-03-06

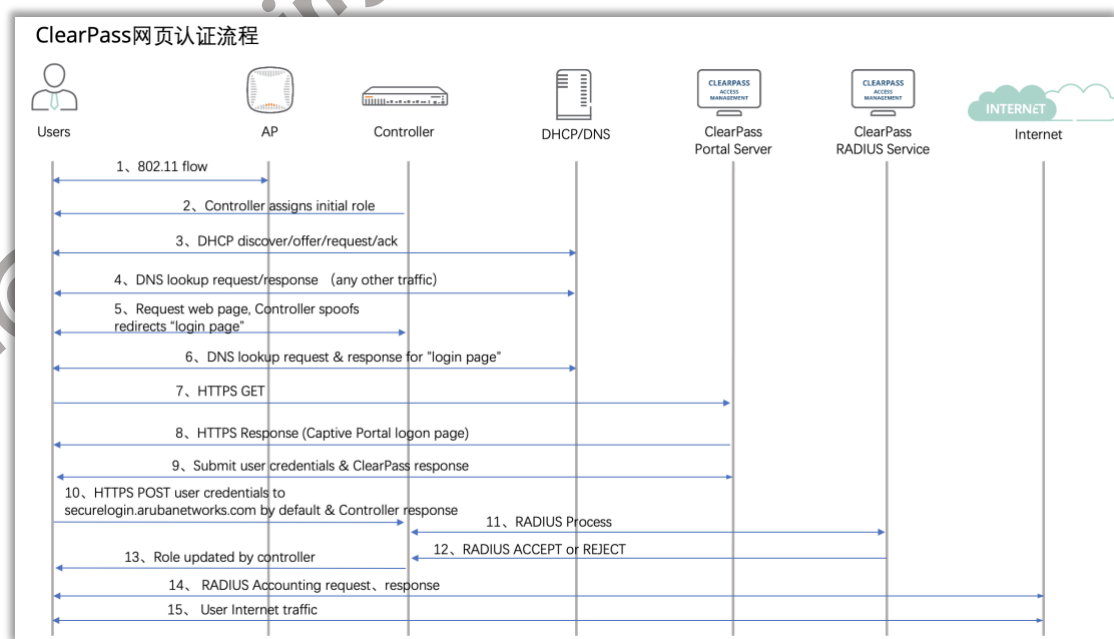
一、网络拓扑图



二、测试目的：

验证 ARUBA 外置 Portal Server 认证中 user post credentials

流程



三、 测试设备：

3.1. 设备型号及版本

设备型号	版本
7010	8.10
ARUAB AP	8.10
ClearPass	6.11
联想笔记本电脑	Win11 25H2

3.2. 测试设备 IP 信息

内容	信息
ClearPass IP	192.168.11.25
无线控制器 IP	10.99.99.99
用户 IP	192.168.110.106
SSID	portal
用户凭证信息	aruba aruba123

四、 测试流程

4.1. 控制器配置内容

4.1.1. ap-group

```
ap-group "default"  
virtual-ap "portal"
```

4.1.2. virtual-ap profile

```
wlan virtual-ap "portal"  
aaa-profile "portal_aaa_prof"  
vlan 110  
ssid-profile "portal_ssid_prof"
```

```
!
```

4.1.3. aaa profile

```
aaa profile "portal_aaa_prof"  
    initial-role "portal-guest-logon"  
    radius-accounting "portal_dot1_svg"  
!
```

4.1.4. SSID Profile

```
wlan ssid-profile "portal_ssid_prof"  
    essid "portal"  
!
```

4.1.5. user-role

```
user-role portal-guest-logon  
    captive-portal "portal_cppm_prof"  
    access-list session global-sacl  
    access-list session apprf-portal-guest-logon-sacl  
    access-list session logon-control  
    access-list session captiveportal  
    access-list session v6-logon-control  
    access-list session captiveportal6  
!
```

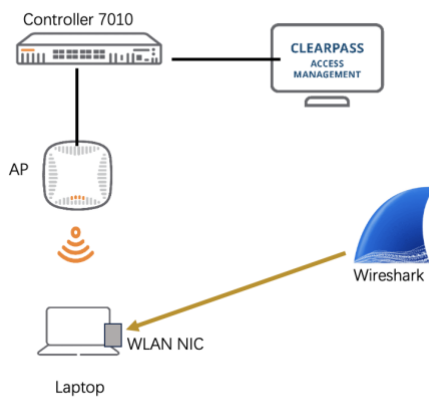
4.1.6. captive-portal profile & auth server

```
aaa authentication captive-portal "portal_cppm_prof"  
    server-group "portal_dot1_svg"  
    protocol-http  
    login-page "http://192.168.110.25/guest/Hello_Baby.php?_browser=1"  
    allow-list "portal_cppm_prof"  
!  
netdestination portal_cppm_prof  
    host 10.99.99.243
```

```
host 192.168.110.25 aaa server-group "portal_dot1_svg"
auth-server 192.168.110.25 position 1
!
aaa authentication-server radius "192.168.110.25"
host "192.168.110.25"
key a4d3fd8e470c7fcd3ddab87a6f02592d6a89e6b49060741f
!
```

4.2. 数据包捕获

4.2.1. 捕获位置：



4.2.2. 捕获周期：

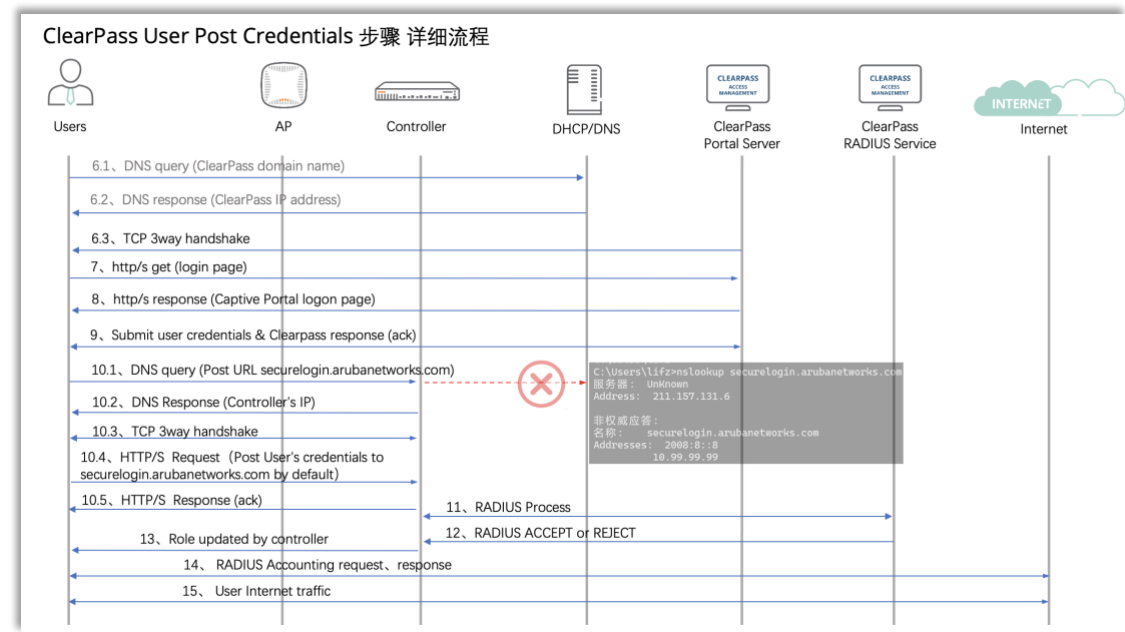
用户连接 WLAN 之前，开启对无线网卡的抓包，直至用户完成认证

流程

4.3. 数据包分析

4.3.1. 详细流程

根据第二章节描述的认证流程，做了详细的流程拆分，以下是流程图：



根据捕获的数据包文件，按照用户接入无线网络的流程先后顺序，对该数据包文件分析：

4.3.2. 客户端获取 IP

用户接入无线网络，SSID： portal，获取 IP。如下所示，客户端经历 discover\offer\request\ack

No.	Time	Source	Destination	Protocol	Length	Info
9	2026-03-06 13:58:46.246797	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x7cc30203
10	2026-03-06 13:58:46.353239	192.168.110.254	192.168.110.106	DHCP	321	DHCP Offer - Transaction ID 0x7cc30203
11	2026-03-06 13:58:46.356089	0.0.0.0	255.255.255.255	DHCP	360	DHCP Request - Transaction ID 0x7cc30203
12	2026-03-06 13:58:46.458975	192.168.110.254	192.168.110.106	DHCP	321	DHCP ACK - Transaction ID 0x7cc30203

4.3.3. 弹出 login page 过程

用户接入网络后，获取了 IP，与 Portal Server 建立 TCP 三次握手

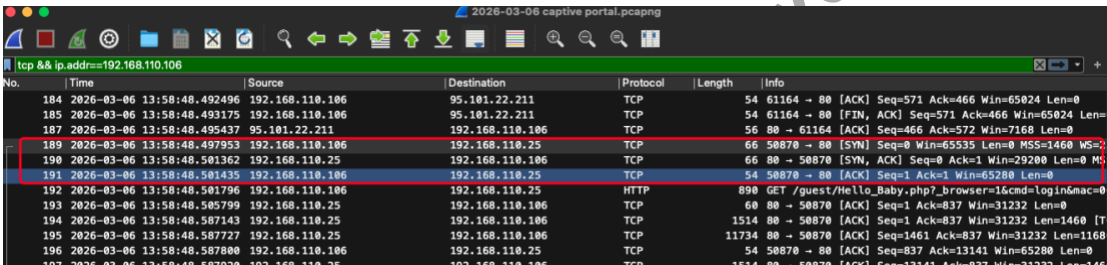
因测试环境是通过 ClearPass 的 IP 直接生成的 login page，如果 ClearPass 更换了 https 证书，则在此步骤前需要 DNS query。

ClearPass https 证书分为 ECC、RSA 两种。更换 RSA 证书需提前 disable https ECC 证书。

下图为客户端与 ClearPass 三次握手截图：

ClearPass IP	192.168.11.25
用户 IP	192.168.110.106

报文序号：189、190、191，对应流程图中步骤 6.3

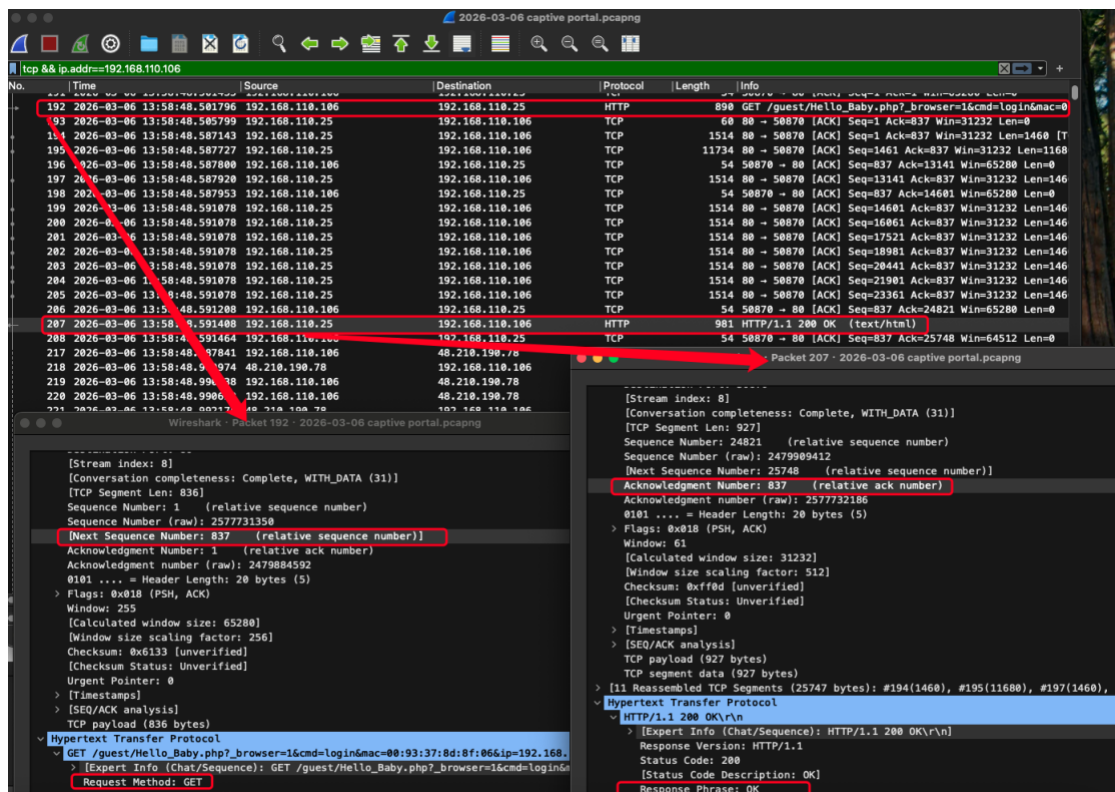


No.	Time	Source	Destination	Protocol	Length	Info
184	2026-03-06 13:58:48.492496	192.168.110.106	95.101.22.211	TCP	54	61164 → 80 [ACK] Seq=571 Ack=466 Win=65024 Len=0
185	2026-03-06 13:58:48.493175	192.168.110.106	95.101.22.211	TCP	54	61164 → 80 [FIN, ACK] Seq=571 Ack=466 Win=65024 Len=0
187	2026-03-06 13:58:48.495437	95.101.22.211	192.168.110.106	TCP	56	80 → 61164 [ACK] Seq=466 Ack=572 Win=7168 Len=0
189	2026-03-06 13:58:48.497953	192.168.110.106	192.168.110.25	TCP	66	50870 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0
190	2026-03-06 13:58:48.501362	192.168.110.25	192.168.110.106	TCP	66	80 → 50870 [SYN, ACK] Seq=0 Ack=1 Win=29280 Len=0 MSS=1460
191	2026-03-06 13:58:48.501435	192.168.110.106	192.168.110.25	TCP	54	50870 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
192	2026-03-06 13:58:48.501796	192.168.110.106	192.168.110.25	HTTP	890	GET /quest/Hello_Baby.php?browser=1&cmd=login&mac=0
193	2026-03-06 13:58:48.505799	192.168.110.25	192.168.110.106	TCP	60	80 → 50870 [ACK] Seq=1 Ack=837 Win=31232 Len=0
194	2026-03-06 13:58:48.507143	192.168.110.25	192.168.110.106	TCP	1514	80 → 50870 [ACK] Seq=1 Ack=837 Win=31232 Len=1460 [T
195	2026-03-06 13:58:48.507727	192.168.110.25	192.168.110.106	TCP	11734	80 → 50870 [ACK] Seq=1461 Ack=837 Win=31232 Len=1168
196	2026-03-06 13:58:48.507800	192.168.110.106	192.168.110.25	TCP	54	50870 → 80 [ACK] Seq=837 Ack=13141 Win=65280 Len=0
197	2026-03-06 13:58:48.507920	192.168.110.25	192.168.110.106	TCP	1514	80 → 50870 [ACK] Seq=13141 Ack=837 Win=31232 Len=1460

4.3.4. 用户“显示”login page

经历 http get、http response，获取网页内容；

报文序号 192、207，对应流程图步骤 7、8



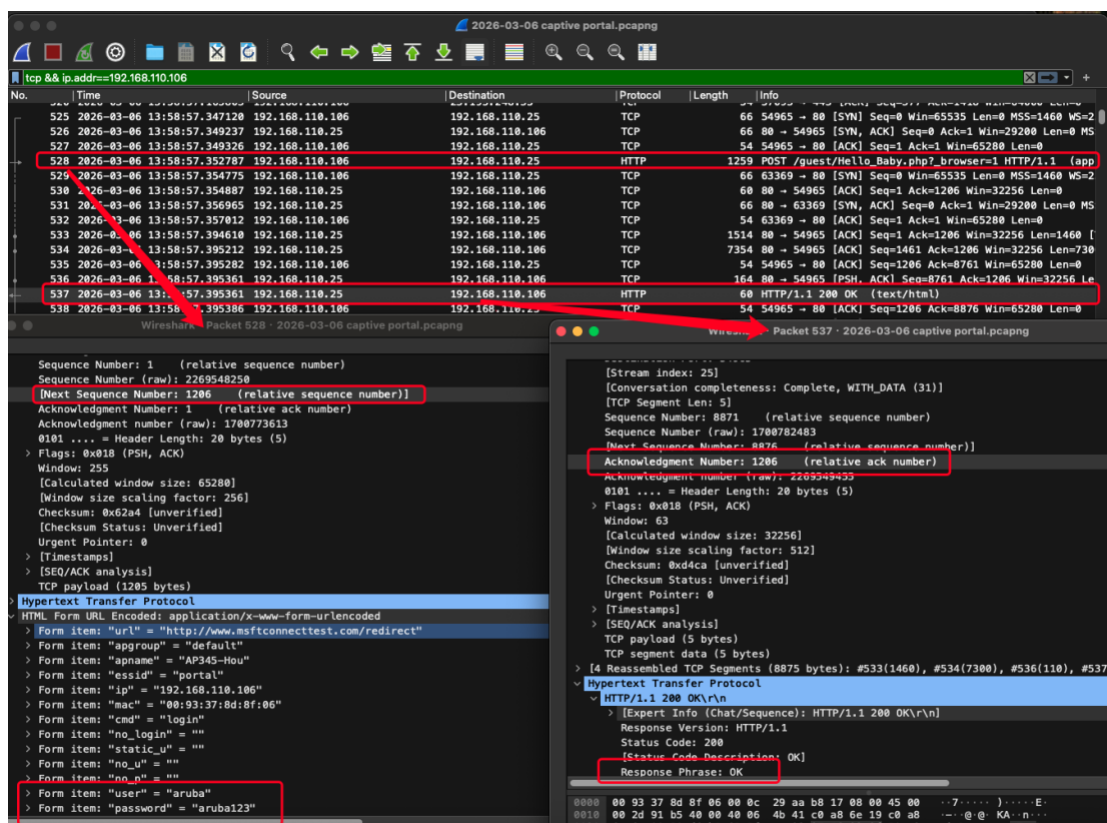
4.3.5. 用户登录

用户在 login page 输入了凭证信息，点击登录

用户凭证信息	aruba aruba123
ClearPass IP	192.168.11.25
用户 IP	192.168.110.106

如下所示，用户向 clearpass post 用户名和密码，clearpass 作 response;

报文序号 528、537，对应流程图 **步骤 9**



4.3.6. 用户 DNS Query Post URL

一般情况下, user post url 为 `http://securelogin.arubanetworks.com`。

如控制器更换了 https 证书, 则前缀变为 `captiveportal-login`,

如下图 8.10.0.0 User Guide 描述:



Server Certificate

The Aruba managed device is designed to provide secure services through the use of digital certificates. The server certificate is installed on the managed device through the Mobility Conductor. A server certificate installed in the managed device verifies the authenticity of the managed devices for captive portal.

Aruba managed device ship with a demonstration self-signed certificate. Until you install a customer-specific server certificate in the managed device, this demonstration self-signed certificate is used by default for all secure HTTP connections such as captive portal. This self-signed certificate is included primarily for the purposes of feature demonstration and convenience and is not intended for long-term use in production networks. Users in a production environment are urged to obtain and install a certificate issued for their site or domain by a well-known CA. You can generate a CSR on the managed device to submit to a CA.

The managed device can accept wild card server certificates (CN begins with an asterisk). If a wildcard certificate is uploaded (for example, CN=*.domain.com), the asterisk in CN is replaced with 'captiveportal-login' in order to derive the Captive Portal logon page URL (captiveportal-login.domain.com).

Once you have imported a server certificate from the Mobility Conductor to managed device, you can select the certificate to be used with captive portal.

Configuring Server Certificate

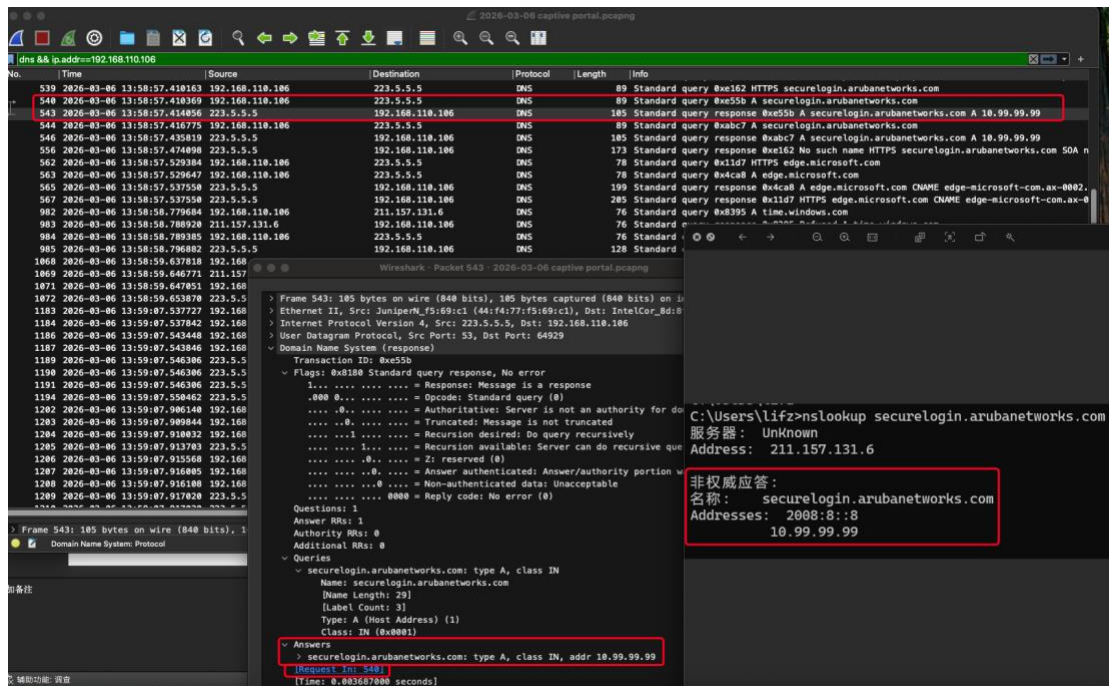
The following procedure describes how to select a certificate for captive portal:

同时也可以可以在命令行查询控制器域名，命令：show datapath fqdn

```
(7010) *[mynode] #show datapath fqdn  
Fri Mar 06 14:53:43.091 2026  
Datapath FQDN Entries  
-----  
securelogin.arubanetworks.com
```

如下图所示：

报文序号 540 543，对应 1 流程图步骤 10.1、10.2

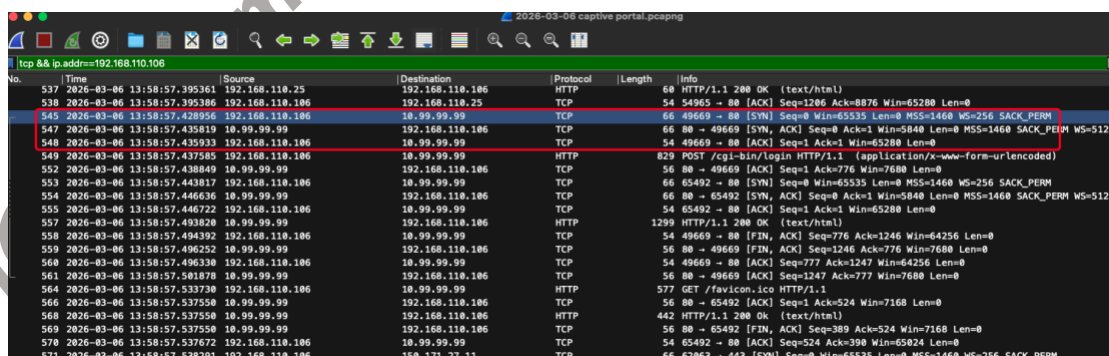


4.3.7. 用户与无线控制器 TCP 三次握手

在用户发起 HTTP Post 之前需要进行 TCP 三次握手

报文序号 545、547、548，对应流程图步骤 10.3

如下截图所示：

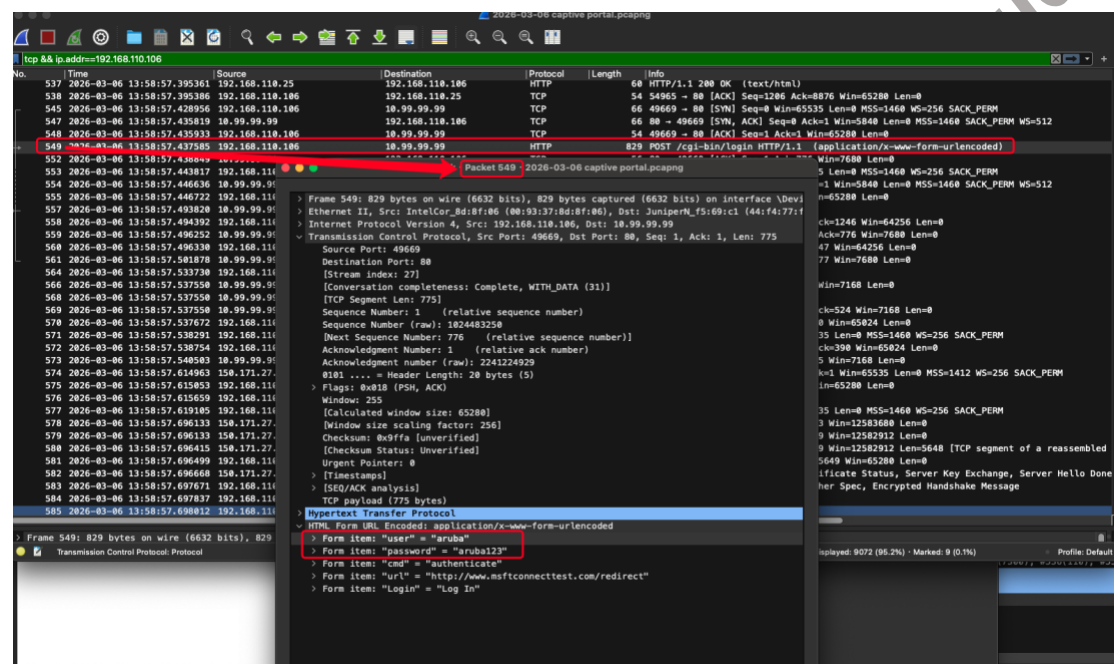


4.3.8. 用户发起 HTTP Post

用户通过 http 协议通过 post 方式将凭证信息发至控制器

报文序号 549, 对应流程图 [步骤 10.4](#)

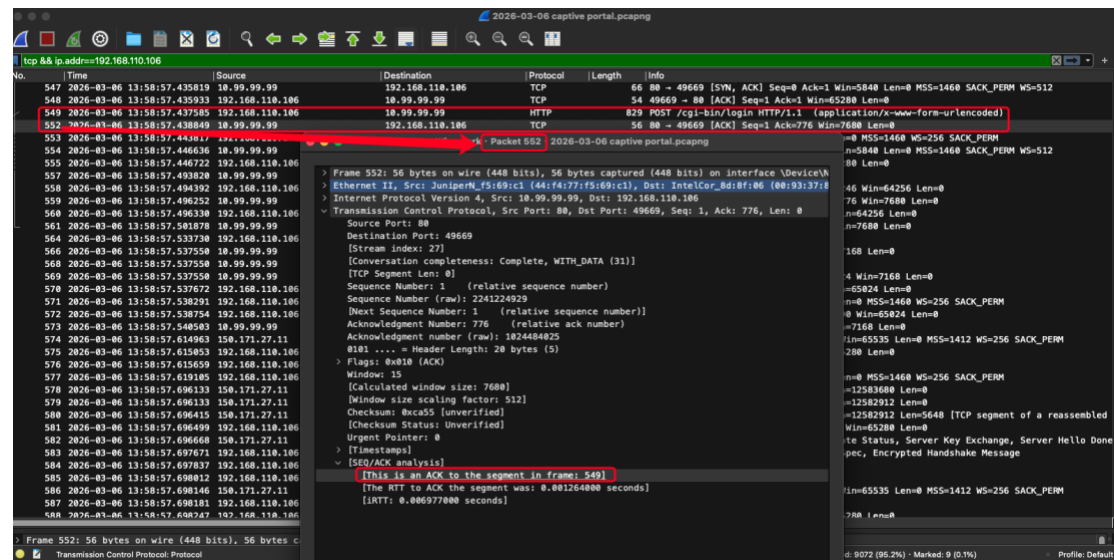
如下图所示



4.3.9. 控制器回应用户 ack

控制器收到用户 http post 的凭证信息后, 回应用户 ack

报文序号 552, 对应流程图 [步骤 10.5](#)



综上，流程一致。