Auto Provision 的使用说明

版本：<1.1>

发布日期：<2018-5-11>

目录

1 介绍

1.1 概述

1、模块说明

自动部署是指，终端获得已存放配置文件的服务器地址以及自动部署的其它参数，之后从对应的服务器上下载配置文件、解析并将配置文件保存到终端本地，从而进行其它更新，例如 firmware 更新等。

2、应用场景

主要应用于工厂给大批量话机进行配置的升级更新。

3、优点

能通过配置文件远程同时升级大批量话机，节省时间人力。

1.2 操作流程概述

方位终端支持 sip PnP、DHCP option、Static Provisioning Server、TR069 四种方式获得自动部署应用参数。如果同时配置了这四种方式，终端启动时将按照四种方式的优先级去选择升级方式。

传输协议支持：ftp、tftp、http、https。

流程：

1. 编辑配置文件修改想要更新的内容，放到相应的服务器目录下并保证服务器开启。
2. 登录网页或 LCD（某些话机不支持 LCD）编辑，启动想要获取自动部署参数的方式（如：sip PnP、DHCP option、Static Provisioning Server、tr069）
3. 重启话机，话机会通过启动的方式获取到带有存放配置文件的服务器地址的 URL
4. 话机解析该 URL 去相应服务器下载配置文件，通常是两个配置文件，通用配置文件和设备配置文件，只有指定的设备配置配置文件名字和通用配置文件名称相同的时候只下载一个。
5. 待配置文件成功下载到话机缓存区，校验该配置与本话机已有的配置文件是否相同，相同则放弃升级，不同则更新该配置文件。
6. 检测新配置是否启动新的下载项 如：版本 、电话本、证书 ，有则启动任务去下载相应下载项。
7. 流程结束。

1.3 术语表

术语名称	解释
PnP	Plug and Play
MACAddress	MAC(Media Access Control)地址，或称为 MAC 位址、硬件位址，用来定义网络设备的位置。在 OSI 模型中，第三层网络层

	负责 IP 地址，第二层数据链路层则负责 MAC 位址。因此一个主机会有一个 IP 地址，而每个网络位置会有一个专属于它的 MAC 位址。
DHCP	动态主机设置协议（Dynamic Host Configuration Protocol，DHCP）是一个局域网的网络协议，使用 UDP 协议工作，主要有两个用途：给内部网络或网络服务供应商自动分配 IP 地址，给用户或者内部网络管理员作为对所有计算机作中央管理的手段。
FTP	文件传输协议（FTP:File Transfer Protocol）使得主机间可以共享文件。 FTP 使用 TCP 生成一个虚拟连接用于控制信息，然后再生成一个单独的 TCP 连接用于数据传输。控制连接使用类似 TELNET 协议在主机间交换命令和消息。文件传输协议是 TCP/IP 网络上两台计算机传送文件的协议，FTP 是在 TCP/IP 网络和 INTERNET 上最早使用的协议之一，它属于网络协议组的应用层。FTP 客户机可以给服务器发出命令来下载文件，上传文件，创建或改变服务器上的目录。
HTTP	超文本传输协议 (HTTP-Hypertext transfer protocol) 是一种详细规定了浏览器和万维网服务器之间互相通信的规则，通过因特网传送万维网文档的数据传送协议。
HTTPS	HTTPS（全称：Hypertext Transfer Protocol over Secure Socket Layer），是以安全为目标的 HTTP 通道，简单讲是 HTTP 的安全版。即 HTTP 下加入 SSL 层，HTTPS 的安全基础是 SSL，因此加密的详细内容就需要 SSL。 它是一个 URI scheme（抽象标识符体系），句法类同 http:体系。用于安全的 HTTP 数据传输。https:URL 表明它使用了 HTTP，但 HTTPS 存在不同于 HTTP 的默认端口及一个加密/身份验证层（在 HTTP 与 TCP 之间）。
TFTP	TFTP（Trivial File Transfer Protocol,简单文件传输协议）是 TCP/IP 协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务。端口号为 69。
URL	统一资源定位符（URL，英语 Uniform Resource Locator 的缩写）也被称为网页地址，是因特网上标准的资源的地址。
AES	AES (Advanced Encryption Standard)采用的一种区块加密标准。
ACS	自动配置服务器(Auto-Configuration Server)。这是在宽带网络中负责客户终端设备自动配置，以实现高级服务的组成要素。
CPE	客户端设备(Customer Premise Equipment)，如支持 TR069 的话机

2 详细分类

2.1 配置文件分类

1、 按功能分类

- 通用配置文件
- 自定义命名的配置文件
- 以 mac 地址命名的配置文件

2、 按格式分类

- xml 格式
- cfg 格式
- txt 格式

3、 按是否加密分类

- 不加密的配置文件
- 加密的配置文件

2.2 自动部署的下载方式

DHCP Option、PnP、Static Provisioning Server、TR069

2.3 自动部署下载方式的优先级

DHCP Option、PnP、Static Provisioning Server、TR069，根据话机的配置不同会有所改变，目前 Android 话机不可改变优先级-其优先级顺序为：MDNS、FDPS、DHCP、TR069、SIP、FLASH

2.4 自动部署的下载协议

tftp、ftp、http、https

2.5 自动部署支持下载的文件类型

4、 firmware、phonebook、etc、Background、mmiset(android 话机现在不支持 mmiset)

2.6 自动部署操作顺序

正确书写配置文件——配置传输协议服务器——进入话机设置下载的方式——重启设备——获取配置文件——通过配置文件获取 URL 下载升级文件

3 自动部署所需环境

DHCP Server、SIP PnP，3cx、TR069 服务器、Https 服务器、Http 服务器、TFTP 服务器、FTP 服务器

使用者需要知道，使用相应的协议要配置相对应的服务器

4 自动部署的详情

4.1 配置文件分类的详细介绍及书写规则

1、 按系列分类

1） 通用配置文件

通用的配置文件会对所有终端配置生效。对于通用配置文件，每个型号终端都有各自特殊的命名，通用配置文件名如下：

a） X 系列低端彩屏、H 系列、门禁系列命名是：f0 型号硬件版本.100.cfg，

例：

话机型号	通用配置文件名称
X1	f0X1hw1.100.cfg
X2	f0X2hw1.100.cfg
X3S	f0X3Shw1.100.cfg
X4	f0X4hw1.100.cfg
H2S	f0H2Shw1.100.cfg
H3	f0H3hw1.100.cfg
H5	f0H5hw1.100.cfg
i16V	f0i16Vhw1.100.cfg
i20S	f0i20SVhw1.100.cfg
i30	f0i30hw1.100.cfg
i23S	f0i23Shw1.100.cfg
i31S	f0i31Shw1.100.cfg
i12	f0i12hw1.100.cfg
i18S	f0i18Shw1.100.cfg
PA2	f0PA2hw1.100.cfg
i13W	f0i13Whw1.100.cfg
I32V	f0i32Vhw1.100.cfg
I33V	f0i33Vhw1.100.cfg
IW30	f0iW30hw1.100.cfg

话机型号	通用配置文件名称
EIM-01	f0EIM-01hw1.100.cfg

b) X 系列高端彩屏命名为：

第一位，公司名字首字母， F

第二三位，终端系列名，默认 V

第四到七位，终端型号

第八到十二位，预留，默认都是 0

例：

话机型号	通用配置文件名称
X5S	F0V0X5S00000.cfg
X6	F0V00X600000.cfg
X7	F0V00X700000.cfg
X7C	F0V0X7C00000.cfg
X210	F0VX21000000.cfg
X210i	F0VX210i00000.cfg

c) Android 话机：

以 f 开头，第二到第三这两位数表示终端的系列名，第四到第七这四位数表示终端的型号，后四位数表示硬件版本号。（现阶段还未区分硬件版本号）

例：

话机型号	通用配置文件名称
F600	f0F06000000.cfg
C600	f0C06000000.cfg
C400	f0C04000000.cfg

d) XU 系列高端彩屏电话机:

话机型号	通用配置文件名称
X3U	F0V0X3U00000.cfg
X4U	F0V0X4U00000.cfg
X5U	F0V0X5U00000.cfg

话机型号	通用配置文件名称
X6U	F0V0X6U00000.cfg

通用配置文件对终端大批量进行自动配置部署有帮助，例如，如果要给 1000 台 X6 所有终端自动部署 firmware，仅仅需要一个带有部署 firmware 参数的 F0V00X600000.cfg，把这个配置文件放在自动配置服务器上就可以了。

2）自定义命名的配置文件

用户可以自定义配置文件名称，如用户指定设备配置文件名称为 name.cfg，那么话机就会去服务器请求下载通用配置文件和 name.cfg，用户可自主输入相应的配置文件名称从服务器上下载要升级的配置。

3）以 mac 地址命名的配置文件

以终端 mac 地址为文件名的配置文件则仅对对应的 mac 地址的终端有效。以 mac 地址为文件名的配置文件就是去掉连接符的 mac 地址。例如，X6 终端的 MAC 地址是 00:15:65:11:3a:f8，以 mac 地址为文件名的配置文件名就是 001565113af8.cfg。用户可以通过此文件去升级指定的话机。

2、按格式分类

1）文件格式支持 cfg、txt、xml

2）文件内部格式

- 文件头 64 字符长度，最后后面是一个回车符即一个\r\n

例：“ <<VOIP CONFIG FILE>>Version:2.0002 ”

注意文件头中的“Version：2.0002”，如果通过 autoprovision 方式升级成功会将版本号（如 2.0002）显示在 web 上相应配置文件版本号位置，如果没有携带 Version：升级成功在 web 上会显示该配置文件的 digest。

- 文件尾部

例：“<<END OF FILE>>”

要更新某个选项一定要把该选项属于的模块头带上

如：你要修改“Host Name :”一定要把“<GLOBAL CONFIG MODULE>”带上，例：

<<VOIP CONFIG FILE>>Version:2.0002

<GLOBAL CONFIG MODULE>

Host Name :VOIP（不小于 20 个字符长度）

<<END OF FILE>>

3、按是否加密分类

1）不加密的配置文件

不加密的配置文件，以明文显示

```
<<VOIP CONFIG FILE>>Version:2.0002

<GLOBAL CONFIG MODULE>

Time Zone           :32

<AUTOUPDATE CONFIG MODULE>

Auto Pbook  Url     :tftp://123:123@172.16.6.70/500.csv
Auto Image Url      :http://123:123@172.16.6.70:8000/x4.z
Auto Etc Url        :tftp://172.16.6.70/sips.pem

<<END OF FILE>>
```

图 1

2）加密的配置文件

- 加密后的配置文件不以明文显示，如图 2：

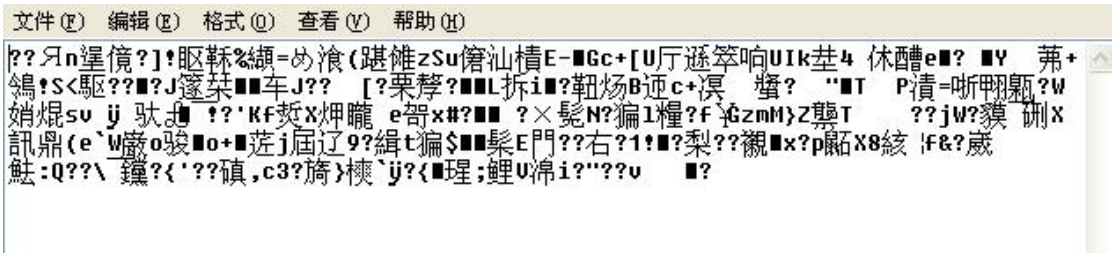


图 2

如果下载的配置文件是通过 AES 加密的，则需要 AES 密钥进行解密。密钥必须是 64 个字符，密钥内容可以使用的字符是 16 进制数字字符（0~F）。所有配置文件都可以进行加密。对应密钥需要填写在 登录 web->MAINTENANCE->AUTO PROVISION 下的 config Encryption Key（下载加密的通用配置文件，密匙填写在此处） 和 Common Config Encryption Key（下载加密的其他配置文件，密匙填写在此处）（如图 3 红线圈起部分）。需要注意的是如果配置文件没有加密，但是你在对应配置文件密钥位置填写密钥，话机也会把它当成已经加密的文件处理

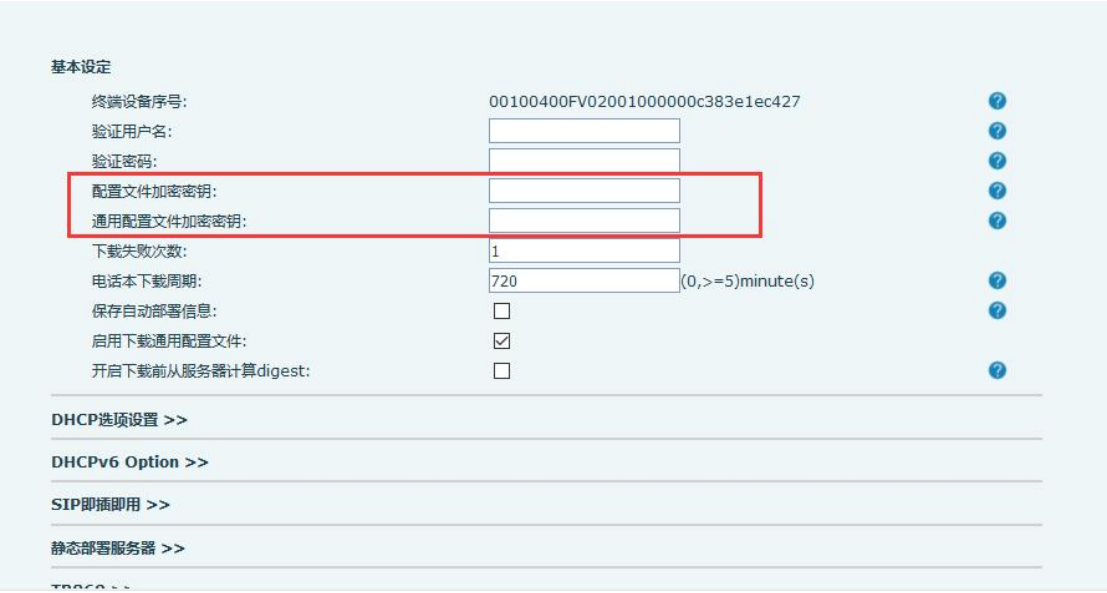


图 3

4.2 URL 的详细介绍

4.2.1 URL 格式

1、话机 url 格式

URL 是 DHCP Option 和 Sip PnP 通过服务器获取到的信息，

1)话机 url 格式是 ：

Server protocol://user:password@Server IP:port/path/Configuration name.

例如 http://user:password@172.16.1.3:8080/X4/$mac.cfg

4.2.2 URL 解析

1、下面详细介绍各部分的功能和设置

1）Server Protocol：服务器使用的传输协议，我们支持 ftp、tftp、http、https 协议。此项必有。

2）User 和 Password 是向服务器请求时候需要的用户名和密码，此项并非必填的项，如登录服务器不需要用户名和密码或者在话机网页上填写（WEB->MAINTENANCE->AUTO PROVISION 如图 4 红线圈起部分填写），如果服务器需要用户名和密码而你忘记填写用户名和密码或网页填写错误，话机会在 LCD 上要求你重新输入用户名和密码，再错还会让你再次输入除非正确或放弃升级。

不填写用户名和密码 URL 格式： Server protocol:// Server IP:port/path/Configuration name

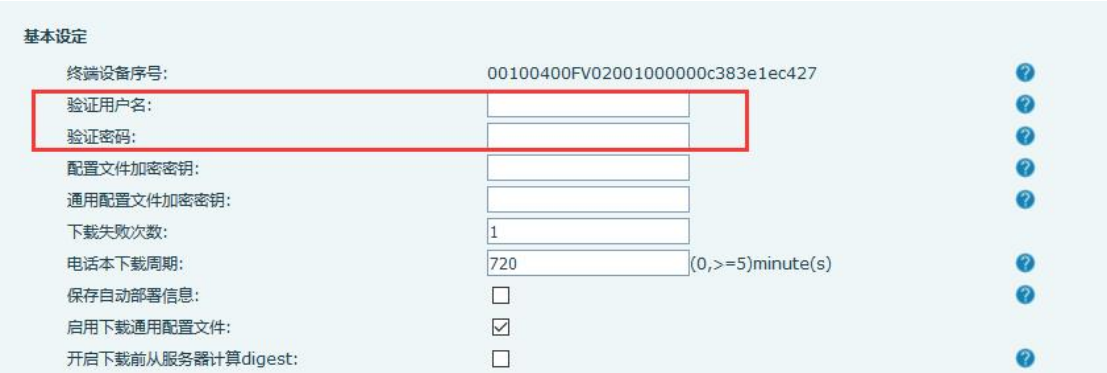


图 4

3）Server Ip 服务器的地址 如 172.16.1.3 。此项必有

4）Port 服务器的端口号，如 8080 ，此项不是必须有，只有服务器自定义了特殊的端口号时候才填写。

不填写端口号 URL 格式：Server protocol:// Server Ip/path/Configuration name

5）Path 配置文件存放的路径，如果存在二级或三级目录此项必填。

6）Configuration name：配置文件名称。这里所指的是设备配置文件名称，通用配置文件的名称是不可变的。该选项有四种写法，如下所示

此项可以不填，不填默认就是下载以 mac 地址命名的设备配置文件（mac.cfg）。

- 写成$mac.cfg，这种写法也是下载以 mac 地址命名的设备配置文件（$mac.xml/$mac.txt）。
- 写成$input.cfg，这个意思是让用户自己手动在 LCD 上输入设备配置文件名称。（$input.xml/$input.txt）
- 最后一种就是指定设备配置文件名称，如 name1.cfg 或 name2.cfg 等

4.3 下载方式的详细介绍

1、DHCP Option

1）使用 DHCP Option ，话机的网络模式必须是 DHCP。

2）DHCP Option 有四个选项可选 分别是 DHCP option 66 、DHCP option 43 、Custom DHCP Option、 DHCP Option Disable

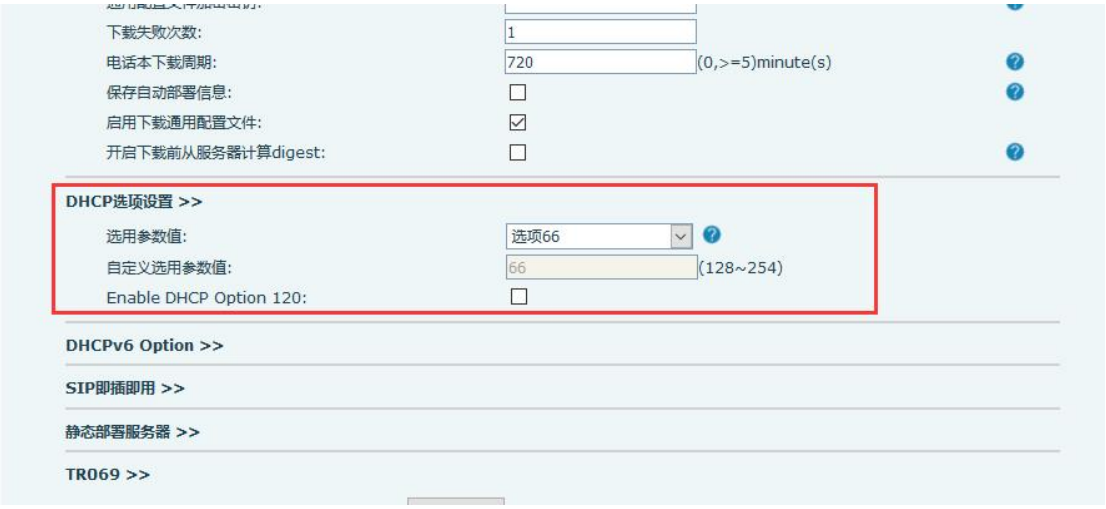


图 5

3）Custom DHCP Option 的设置范围是 128~254， DHCP Option Disable 关闭 DHCP Option。

设置完毕之后重启话机或者等待 DHCP 续租时话机会向 DHCP 服务器请求 option 信息，如果服务器设置回复你请求的 option 信息，就会在服务回复的抓包中查看到对应 option 信息（过滤 bootp，查看 ACK 包）得到 URL，话机解析这个 URL，在通过 DHCP 方式获得自动部署应用参数时，用户可任选其中一种。例如，在通过 DHCP 方式获得自动部署应用参数时选择 DHCP option 43，在终端向服务器发的 DHCP discover message 和 DHCP request message 中会有如下字段值：

Option: (t=55,l=7) Parameter Request List

Option: (55) Parameter Request List

Length: 7

Value: 011c0302042b06

1 = Subnet Mask

28 = Broadcast Address

43 = Vendor-Specific Information

在服务器向终端发的 DHCP offer message 和 DHCP ACK message 中会有如下字段值：

Option: (t=43,l=29) Vendor-Specific Information

Option: (43) Vendor-Specific Information

Length: 29

Value: 746674703a2f2f3139322e3136382e312e3131382f246d61...

Option: (t=43,l=29) Vendor-Specific Information 信息中的 Value 值就是要下载配置文件 URL 路径的十六进制形式。即 Value 值就是 http://172.16.6.45/$mac.cfg。方位终端支持$mac 替换，其 Value 值 URL 可以是 http://ip/$mac.cfg 也可以是 http://ip/mac.cfg?mac=$mac.cfg 。

DHCP option 66 和 DHCP custom option 应用参数同上述 DHCP option 43。

注意：

方位终端也支持 http://ip/$input.cfg URL 形式。如果上述的 Option: (t=43,l=29) Vendor-Specific Information 信息中的 Value 值是 http://172.16.6.45/$input.cfg，那么在话机终端会弹出输入终端对应配置 ID 值的对话框，这个终端对应配置 ID 值是由管理员分配的。用户在输入终端对应配置 ID 后，终端就会自动从服务器下载终端对应 ID 配置文件。同样方位终端$input 替换，其 Value 值 URL 可以是 http://ip/$input.cfg 也可以是 http://ip/input.cfg?input=$input.cfg 。

4）操作方法

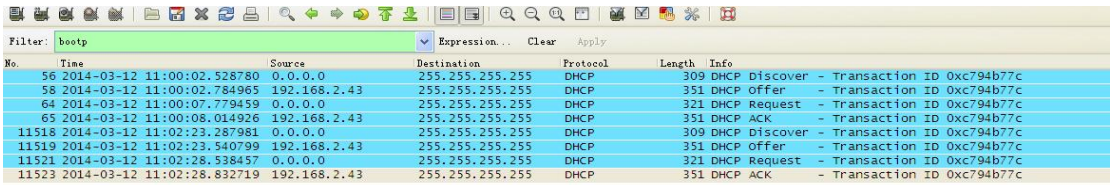
a）以 dhcp option 66 为例

- 话机网络模式为 DHCP
- 登陆话机 web 页面，进入管理设置，选择 dhcp option 66
- 断开外网，开启 DHCP SERVER，打开 dhcpsrv.ini，设置要升级的 url
- 将要下载的配置文件放于服务器的对应目录下。
- 重启话机，抓包。
- 例如：配置的 url 是使用 tftp 服务器去下载自定义的 xml 格式的配置文件，配置文件设置如下：

```
<VOIP CONFIG FILE>
<Digests>2.0002</Digests>
<GLOBAL CONFIG MODULE>
<Time_Zone>32<Time_Zone>
</GLOBAL CONFIG MODULE>
<AUTOUPDATE CONFIG MODULE>
<Auto Image Url> tftp://172.16.6.45/x4.z</Auto Image Url>
</AUTOUPDATE CONFIG MODULE>
</VOIP_CONFIG_FILE>
```

图 6

只下载时区和 image，升级过程中可以抓 bootp、tftp 包查看，相应的服务器也会有显示，如图 6：


Filter: bootp
Expression... Clear Apply
No. Time Source Destination Protocol Length Info
56 2014-03-12 11:00:02.528780 0.0.0.0 255.255.255.255 DHCP 309 DHCP Discover - Transaction ID 0xc794b77c
58 2014-03-12 11:00:02.784965 192.168.2.43 255.255.255.255 DHCP 351 DHCP Offer - Transaction ID 0xc794b77c
64 2014-03-12 11:00:07.779459 0.0.0.0 255.255.255.255 DHCP 321 DHCP Request - Transaction ID 0xc794b77c
65 2014-03-12 11:00:08.014926 192.168.2.43 255.255.255.255 DHCP 351 DHCP ACK - Transaction ID 0xc794b77c
11518 2014-03-12 11:02:23.287981 0.0.0.0 255.255.255.255 DHCP 309 DHCP Discover - Transaction ID 0xc794b77c
11519 2014-03-12 11:02:23.540799 192.168.2.43 255.255.255.255 DHCP 351 DHCP Offer - Transaction ID 0xc794b77c
11521 2014-03-12 11:02:28.538457 0.0.0.0 255.255.255.255 DHCP 321 DHCP Request - Transaction ID 0xc794b77c
11523 2014-03-12 11:02:28.832719 192.168.2.43 255.255.255.255 DHCP 351 DHCP ACK - Transaction ID 0xc794b77c

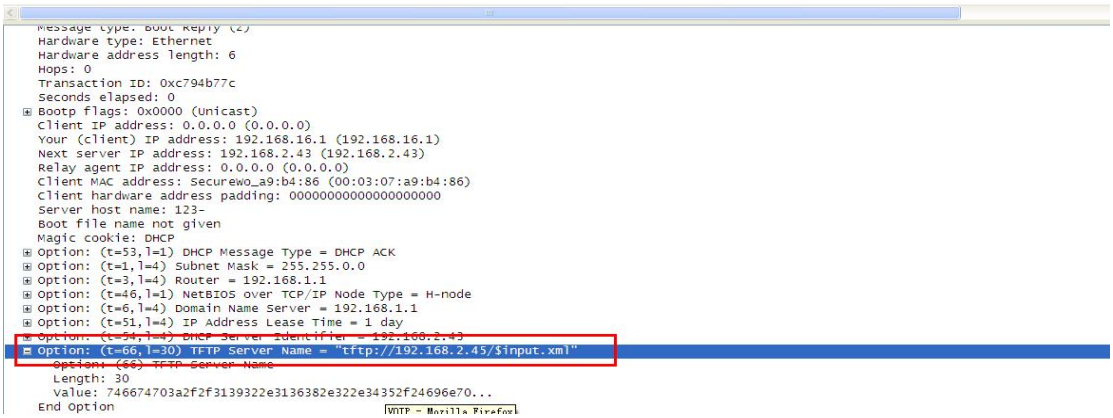

Message type: Boot Reply (2)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0xc794b77c
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 192.168.16.1 (192.168.16.1)
Next server IP address: 192.168.2.43 (192.168.2.43)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Securewo_a9:b4:86 (00:03:07:a9:b4:86)
Client hardware address padding: 00000000000000000000
Server host name: 123-
Boot file name not given
Magic cookie: DHCP
Option: (t=53,l=1) DHCP Message Type = DHCP ACK
Option: (t=1,l=4) Subnet Mask = 255.255.0.0
Option: (t=3,l=4) Router = 192.168.1.1
Option: (t=46,l=1) NetBIOS over TCP/IP Node Type = H-node
Option: (t=6,l=4) Domain Name Server = 192.168.1.1
Option: (t=51,l=4) IP Address Lease Time = 1 day
Option: (t=54,l=4) DHCP Server Identifier = 192.168.2.43
Option: (t=66,l=30) TFTP Server Name = "tftp://192.168.2.45/$input.xml"
Option: (66) TFTP Server Name
Length: 30
Value: 746674703a2f2f3139322e3136382e322e34352f24696e70...
End Option

图 7

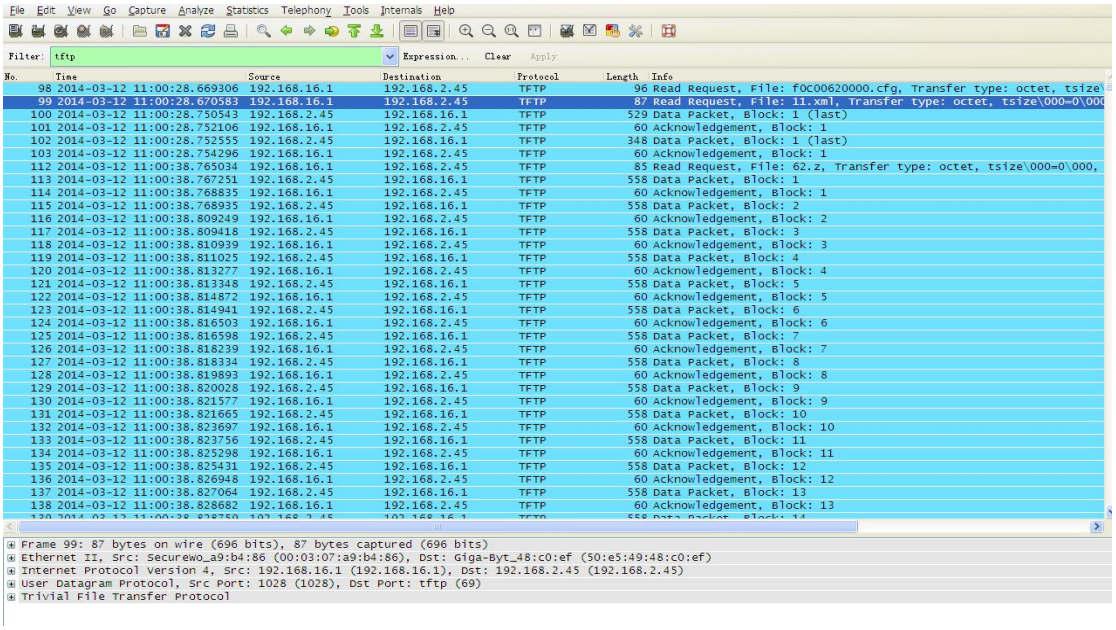

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tftp
Expression... Clear Apply
No. Time Source Destination Protocol Length Info
98 2014-03-12 11:00:28.669306 192.168.16.1 192.168.2.45 TFTP 96 Read Request, File: f0C00620000.cfg, Transfer type: octet, tsize
99 2014-03-12 11:00:28.670583 192.168.16.1 192.168.2.45 TFTP 87 Read Request, File: 11.xml, Transfer type: octet, tsize\000=0\000
100 2014-03-12 11:00:28.750543 192.168.2.45 192.168.16.1 TFTP 529 Data Packet, Block: 1 (last)
101 2014-03-12 11:00:28.752106 192.168.16.1 192.168.2.45 TFTP 60 Acknowledgement, Block: 1
102 2014-03-12 11:00:28.752555 192.168.2.45 192.168.16.1 TFTP 348 Data Packet, Block: 1 (last)
103 2014-03-12 11:00:28.754296 192.168.16.1 192.168.2.45 TFTP 60 Acknowledgement, Block: 1
112 2014-03-12 11:00:38.765034 192.168.16.1 192.168.2.45 TFTP 85 Read Request, File: 62.z, Transfer type: octet, tsize\000=0\000,
113 2014-03-12 11:00:38.767251 192.168.2.45 192.168.16.1 TFTP 558 Data Packet, Block: 1
114 2014-03-12 11:00:38.768835 192.168.16.1 192.168.2.45 TFTP 60 Acknowledgement, Block: 1
115 2014-03-12 11:00:38.768935 192.168.2.45 192.168.16.1 TFTP 558 Data Packet, Block: 2
116 2014-03-12 11:00:38.809249 192.168.16.1 192.168.2.45 TFTP 60 Acknowledgement, Block: 2
117 2014-03-12 11:00:38.809418 192.168.2.45 192.168.16.1 TFTP 558 Data Packet, Block: 3
118 2014-03-12 11:00:38.810939 192.168.16.1 192.168.2.45 TFTP 60 Acknowledgement, Block: 3
119 2014-03-12 11:00:38.811025 192.168.2.45 192.168.16.1 TFTP 558 Data Packet, Block: 4
120 2014-03-12 11:00:38.813277 192.168.16.1 192.168.2.45 TFTP 60 Acknowledgement, Block: 4
121 2014-03-12 11:00:38.813348 192.168.2.45 192.168.16.1 TFTP 558 Data Packet, Block: 5
122 2014-03-12 11:00:38.814872 192.168.16.1 192.168.2.45 TFTP 60 Acknowledgement, Block: 5
123 2014-03-12 11:00:38.814941 192.168.2.45 192.168.16.1 TFTP 558 Data Packet, Block: 6
124 2014-03-12 11:00:38.816503 192.168.16.1 192.168.2.45 TFTP 60 Acknowledgement, Block: 6
125 2014-03-12 11:00:38.816598 192.168.2.45 192.168.16.1 TFTP 558 Data Packet, Block: 7
126 2014-03-12 11:00:38.818239 192.168.16.1 192.168.2.45 TFTP 60 Acknowledgement, Block: 7
127 2014-03-12 11:00:38.818334 192.168.2.45 192.168.16.1 TFTP 558 Data Packet, Block: 8
128 2014-03-12 11:00:38.819893 192.168.16.1 192.168.2.45 TFTP 60 Acknowledgement, Block: 8
129 2014-03-12 11:00:38.820028 192.168.2.45 192.168.16.1 TFTP 558 Data Packet, Block: 9
130 2014-03-12 11:00:38.821577 192.168.16.1 192.168.2.45 TFTP 60 Acknowledgement, Block: 9
131 2014-03-12 11:00:38.821665 192.168.2.45 192.168.16.1 TFTP 558 Data Packet, Block: 10
132 2014-03-12 11:00:38.823697 192.168.16.1 192.168.2.45 TFTP 60 Acknowledgement, Block: 10
133 2014-03-12 11:00:38.823756 192.168.2.45 192.168.16.1 TFTP 558 Data Packet, Block: 11
134 2014-03-12 11:00:38.825298 192.168.16.1 192.168.2.45 TFTP 60 Acknowledgement, Block: 11
135 2014-03-12 11:00:38.825431 192.168.2.45 192.168.16.1 TFTP 558 Data Packet, Block: 12
136 2014-03-12 11:00:38.826948 192.168.16.1 192.168.2.45 TFTP 60 Acknowledgement, Block: 12
137 2014-03-12 11:00:38.827064 192.168.2.45 192.168.16.1 TFTP 558 Data Packet, Block: 13
138 2014-03-12 11:00:38.828682 192.168.16.1 192.168.2.45 TFTP 60 Acknowledgement, Block: 13
Frame 99: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)
Ethernet II, Src: Securewo_a9:b4:86 (00:03:07:a9:b4:86), Dst: Giga-Byt_48:c0:ef (50:e5:49:48:c0:ef)
Internet Protocol Version 4, Src: 192.168.16.1 (192.168.16.1), Dst: 192.168.2.45 (192.168.2.45)
User Datagram Protocol, Src Port: 1028 (1028), Dst Port: tftp (69)
Trivial File Transfer Protocol

图 8

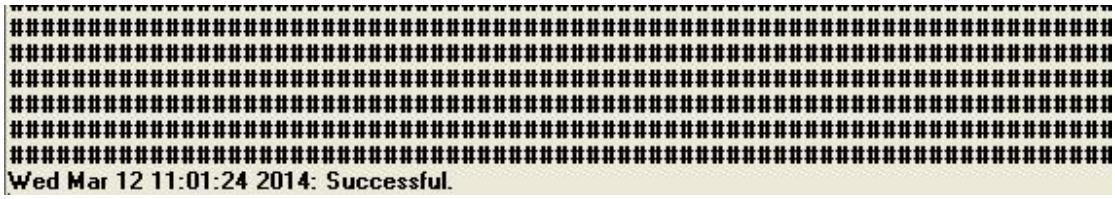


图 9

Option43、Option Custom 也是同样的下载方式，只要在 dhcpsrv.ini 中将 url 进行修改就行。

b）https 升级

由于自己本地搭建的 dhcp server 不支持 https 升级，需要用到 1.3 服务器， 这里单独介绍。操作方法如下（以 option 66 为例）：

- 通过 SecureCRT.EXE telnet 进入服务器的链接，进入 etc 目录，cd /etc
- 打开文件，vi dhcpd.conf
- 回车后按 i 可以编辑修改相应项

图 10

- 修改后按 Esc 退出修改

- 按 Shift+：才能输入保存命令（q！不保存， wq 保存）
- 重启 dhcp 服务器使修改生效，service dhcpd restart
- 将要下载的配置文件放到服务器指定目录下
- 话机选为 option 66
- 重启
- 抓包

bootp 包中携带下载路径，tcp 包中可以看到传输的内容为密文。

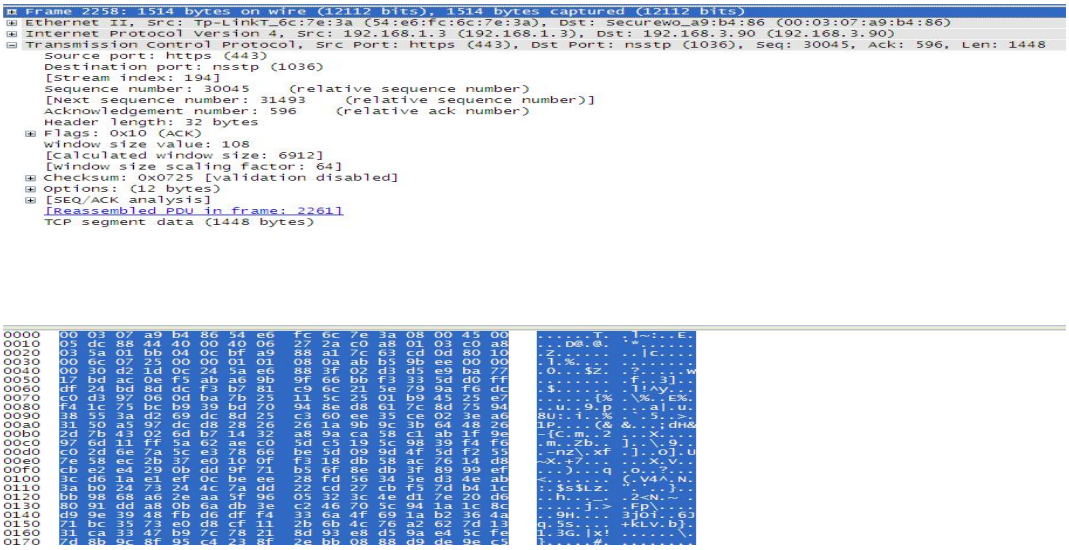


图 11

2、pnp

1）Plug & Play (PnP)（中文为即插即用） 为自动配置部署提供了一种基于 SIP 协议通信的配置升级/部署方法。填入服务器 IP，端口，并且勾选

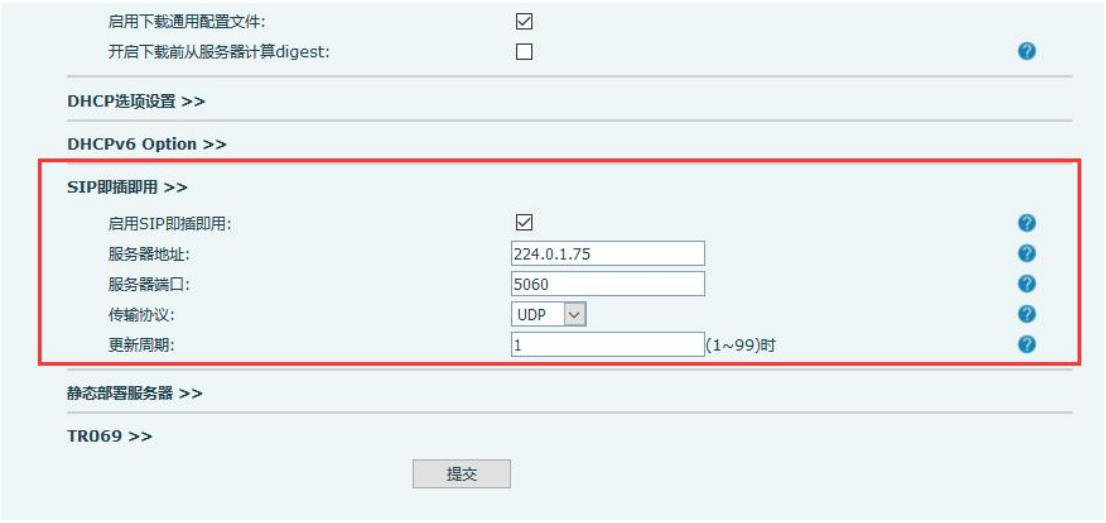
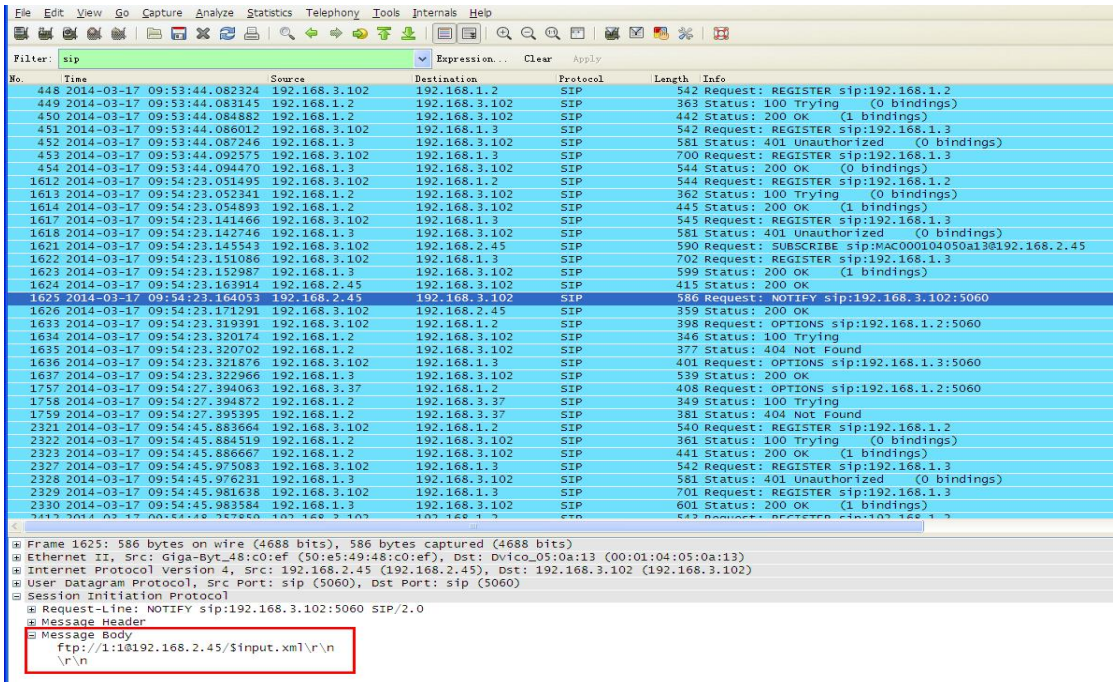


图 12

如果终端开启了启用 PnP 模式，终端启动后它将以组播形式周期性发送 SIP SUBSCRIBE 消息。任何一个兼容支持此特定消息的 SIP 服务器会响应，并回送一个包含自动配置/部署服务器路径的 SIP NOTIFY 消息，通过此路径终端能够获得要下载的配置文件。这种自动配置/部署主要用在一些没有默认自动配置/部署服务器配置，或者终端使用静态 IP，无法通过 DHCP option 进行相关参数自动获取的场景下。在 X4 或者更高版本中，如果终端从 PnP 服务器获取地址参数失败，则会继续其他流程获取。如图 11




```
<![CDATA[

NOTIFY sip:[remote_ip]:5060 SIP/2.0
Via: SIP/2.0/[transport] [local_ip]:[local_port];branch=[branch]
From: [$2]
To: [$1]
[last_Call-ID:]
CSeq: 1 NOTIFY
Max-Forwards: 70
Content-Type: application/url
Subscription-State: terminated;reason=timeout
Event: ua-profile;profile-type="device";vendor="lishuai";model="VOIP PHONE  ";ver
Content-Length:[len]

tftp://172.16.6.45/$input.txt      edit URL become you want in here

]]>
</send>

<recv response="200" crlf="true">
</recv>

</scenario>
```

图 13

2）操作方法（以 3cx 举例子）

登陆话机 web，开启 pnp，填写 pnp 服务器地址，pnp 端口，pnp 协议（udp、tcp），

pnp 周期（一般默认），重启话机

登录 3cx，找到对应话机,下发配置，服务器给话机发 notify，如图

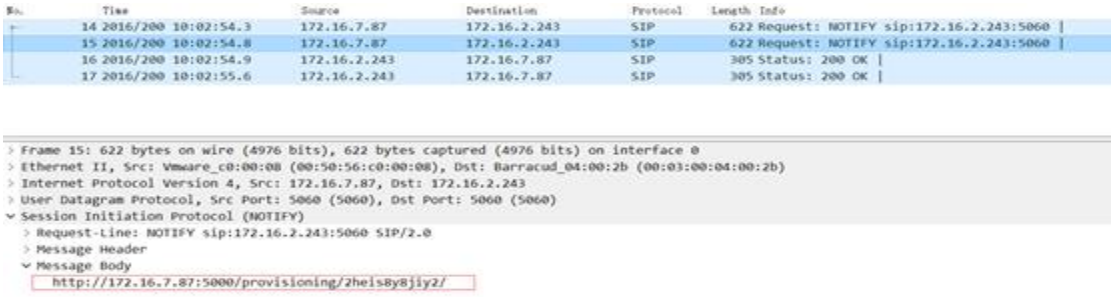


图 14

3 、Static Provisioning Server

1）此流程是通过固定的配置服务器参数进行检测下载。

这个流程取决于检测配置方式的设置，如果检测配置方式是禁用，终端就不会检测保存的配置里的服务器参数并下载。此流程支持 HTTP/HTTPS/FTP/TFTP。此配置的用户名和密码是根据服务器认证需要来通过认证授权。例如，连接 FTP 服务器时就需要首先用户名和密码认证：配置终端的自动配置/部署服务器地址如 172.16.6.45，输入用户名 winline 和密码 winline（在 web 页面是用对应个数的点来隐藏显示），再选择如 FTP 协议，终端在启用了更新检测后，就能依照流程优先级最后访问 FTP 服务器，下载配置。如果终端通过 Static Provisioning Server 下载配置文件失败，则获得自动部署应用参数流程就会停止，终端不再进行自动配置/升级部署流程。

图 15

2）操作方法

- 配置 Static Provisioning Server
- 将配置文件放在服务器对应目录下
- 重启话机

注：当配置文件名称设置为话机的 MAC 地址时。X5/6 系列话机配置静态部署服务器时可以不配置配置文件名。X3/4 系列话机则要确保开启下载自定义配置文件，才可以不配置文件名。

4、TR069

TR069 为 CPE 广域网管理协议。它提供了 CPE 和 ACS 之间的通信。它定义了一个应用层协议的最终用户设备进行远程管理。所以在部署 TR069 之前，我们需要一个有效的 ACS。Fanvil 端点 ACS 支持两种类型，一种是 CTC，另一种是 Common.不同的 ACS，有不同的功能， CTC 支持 XML 格式，Common 支持 SIP 信息和配置文件和固件的配置。如果它被设置为已禁用，话机将无法检测到 TR069。

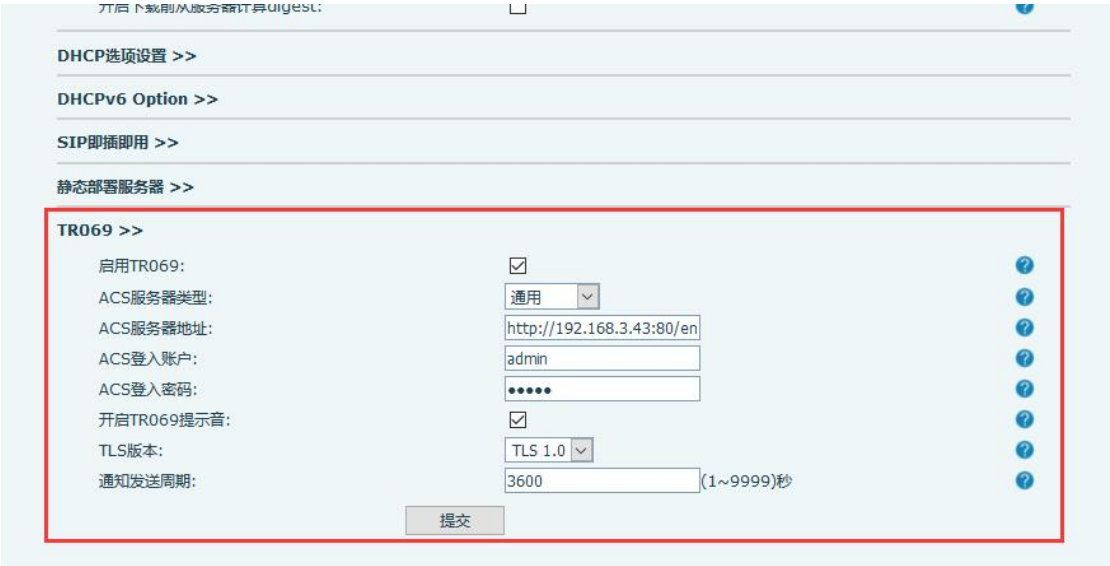
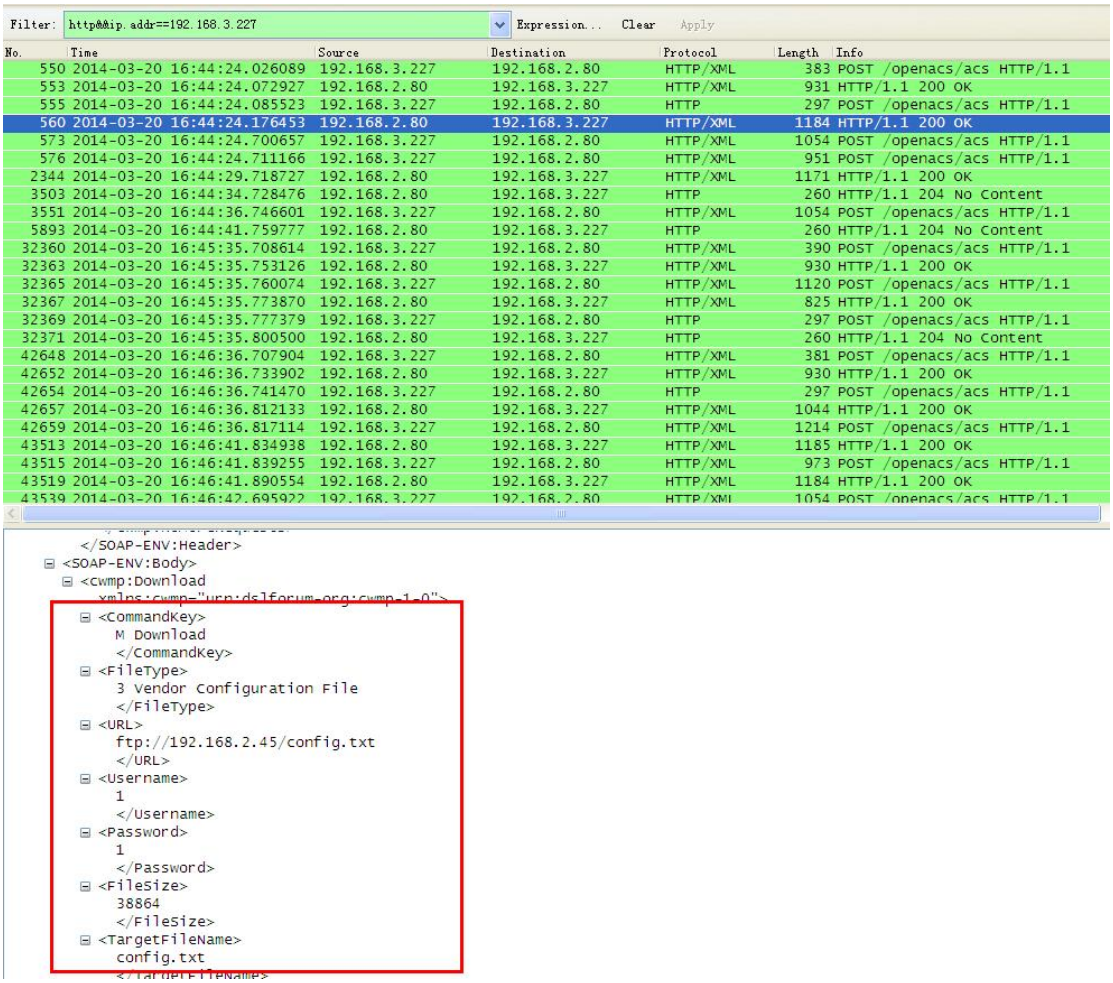


图 16

开启 TR069 重启后，抓 http 包，可以看到话机会先向服务器发一个连接请求，之后会再发一个认证请求，成功的话服务器会分别回复 200 OK,其中认证的 2000K 中带有对话机进行操作的脚本内容。如果想对话机进行相应的操作，要登陆 TR069 服务器（htt http://172.16.1.16:8081/openacs）进行配置

例如：下载配置文件

- 登陆 TR069 服务器，在 Configuration scripts 页面,找到 Download 项,将里面的内容拷贝到 default 项中，根据自身情况更改下载配置文件路径
- 打开相应服务器
- 将相应的配置文件放到指定目录下
- 话机开启 TR069 ，重启
- 重启话机，抓包



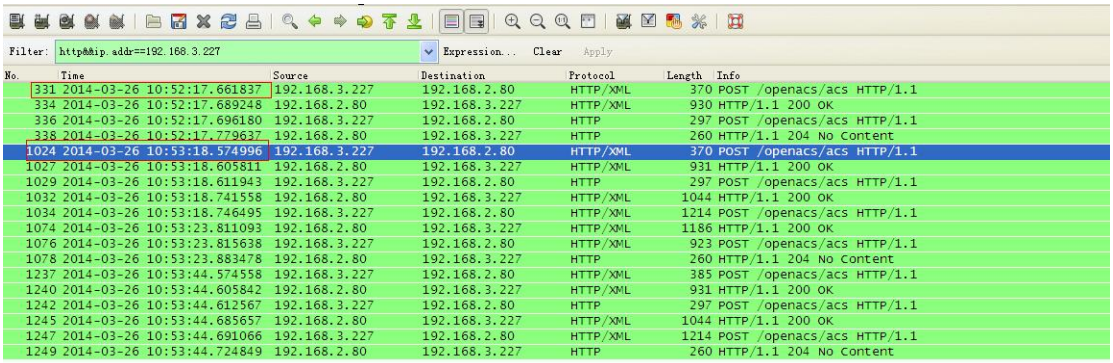


图 17

4.4 支持文件类型的详细介绍

1、firmware

话机的版本，自动部署支持版本的 degist 的比较功能，升级时要改变版本的 degist，否则相同版本不能进行二次下载。

配置文件中的 url 示例（以 txt 格式为例）：

Auto Image Url :ftp://172.16.6.70:8000/x4.z

```
<<VOIP CONFIG FILE>>Version:2.0002

<AUTOUPDATE CONFIG MODULE>

Auto Image Url      :ftp://123:123@172.16.6.70:8000/x4.z

<<END OF FILE>>
```

图 18

2、Phone Book

电话本，有 xml、vcf、csv 三种格式。

Auto Pbook Url :tftp://123:123@172.16.6.70/500.vcf

```
<<VOIP CONFIG FILE>>Version:2.0002

<AUTOUPDATE CONFIG MODULE>

Auto Pbook  Url     :tftp://123:123@172.16.6.70/500.csv

<<END OF FILE>>
```

图 19

3、etc

证书，后缀为.bin、crt、key、xml、pem 都可以。

```
Auto etc Url        :ftp://1:1@172.16.6.70/sips.pem
<<VOIP CONFIG FILE>>Version:2.0002

<AUTOUPDATE CONFIG MODULE>
Auto Etc Url        :tftp://172.16.6.70/sips.pem
<<END OF FILE>>
```

图 20

4、Background

背景图，固定以 background 命名，为 bmp 格式。

```
Auto Logo Url       :tftp://172.16.6.70/background.bmp
<<VOIP CONFIG FILE>>Version:2.0002

<AUTOUPDATE CONFIG MODULE>
Auto Logo Url       :tftp://172.16.6.70/background.bmp
<<END OF FILE>>
```

图 21

5、 Mmiset

mmiset 包含话机所有的网页和定制信息，话机的自动部署不支持.mmiset 的格式，要将其打包成.z 的格式再去升级。

```
Auto Mmiset Url:
tftp://123:123@172.16.6.45/mmiset6_SpanishT20131206171925.z
<<VOIP CONFIG FILE>>Version:2.0002

<AUTOUPDATE CONFIG MODULE>
Auto Mmiset Url     :tftp://123:123@172.16.6.45/mmiset6_SpanishT20131206171925.z
<<END OF FILE>>
```

图 22

6、 Dialpeer.csv(只有行业支持)

拨号规则，固定以 dialPeer 命名，为 csv 格式。

```
Auto DPeer Url :ftp://123:123@172.16.6.45:8080/dialPeer.csv

<<VOIP CONFIG FILE>>Version:2.0002

<AUTOUPDATE CONFIG MODULE>

Auto DPeer Url :ftp://123:123@172.16.6.45:8080/dialPeer.csv

<<END OF FILE>>
```

图 23

7、 Access table(只有门禁系列支持型号有 i31s、i30、i23s、i20s、i32v、i33V)

自动升级门禁访问列表,固定以 accessList 命名，为 csv 格式

Auto AList Url :ftp://123:123@172.16.6.45:8080/accessList.csv

```
<<VOIP CONFIG FILE>>Version:2.0002

<AUTOUPDATE CONFIG MODULE>

Auto AList Url  :ftp://123:123@172.16.6.45:8080/accessList.csv

<<END OF FILE>>
```

图 24

4.5 保存自动部署信息的应用

在 web 页面勾选此项，如图 25：

图 25

如果话机使用自定义配置文件升级,第一次升级时话机会弹出输入配置文件 ID 的提示框，输入后话机去进行下载，第二次再升级此配置文件，话机会记住之前的 ID 不会再提示输入，而是直接去下载。

〈*注 1: 自动部署最新修改，配置文件内部格式不做限制〉

〈*注 2:相同配置文件不能连续下载两次，要做些改变，如改时区或是加几行空格〉

〈*注 3:相同版本不能连续下载两次，要改变版本的 degest〉

〈*注 4:以前的自动升级分为 version 和 digest 两种方式，其中以 versin 开头的配置文件区分配置文件版本号，要版本号大于话机当前的才能升级，而 digest 格式不用区分。现在的升级都不做区分〉

4.6 自动升级门禁访问列表说明

首先点击导出门禁访问列表，在表格里面编辑需要导入的信息，通过自动升级的方式升级列表，升级成功后，可在门禁访问列表中看到导入详情。

图 26