Grandstream Networks, Inc.

XML 自动配置指南

GXV3140/GXV3175 多媒体 IP 电话
GXV21XX/GXP14XX 企业级 IP 电话
HT50x 模拟电话适配器
GXW40xx FXS 模拟 IP 网关

目录

概述

XML 自动配置系统允许潮流网络 IP 电话通过 XML 配置文件进行统一配置更新。此外，XML 自动配置在执行过程中允许一般配置文件的优先级高于基于 MAC 地址的配置文件。

说明：XML 自动配置目前支持以下几款潮流网络公司产品：

- GXV3140 多媒体 IP 电话
- GXV3175 多媒体 IP 电话
- GXP21XX/GXP14XX 企业级 IP 电话
- HT50X 模拟电话适配器
- GXW40XX FXS 模拟 IP 网关

自动配置流程

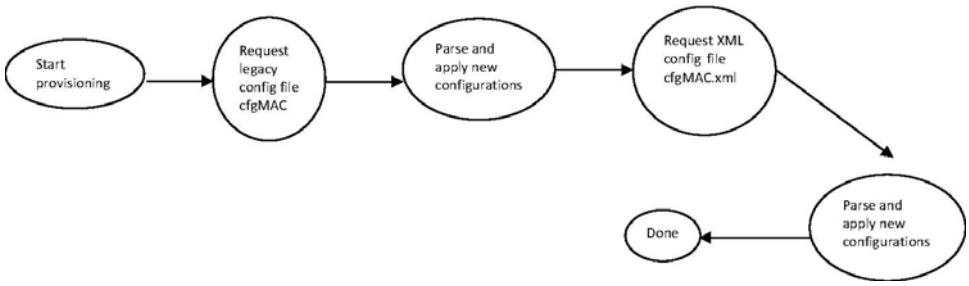

图1. 自动配置流程

下载完原有的二进制 cfgMAC 配置文件后，设备中的自动配置程序将会重新加载并应用此文件中的新设置，即自动配置/重定向服务器在不重启设备的条件下，可以将设备重定向至 XML 自动配置服务器。此功能也可以用于发送 XML 文件加密密码。

XML 文件结构和示例

常规的XML句法是由一列**名称-值**的标记对组成的，其中P值是关键要素。P值的取值就是对P值所代表的参数配置的参数值。如需了解详细的P值表，请参考原有的配置模板，下载地址为：http://www.grandstream.com/index.php/support/tools。

XML 配置文件举例（cfgxxxxxxxxxxxx.xml）

```
<?xml version="1.0" encoding="UTF-8" ?>
<gs_provision version="1">
  <mac>000b82123456</mac>
  <config version="1">
    <P271>0</P271>
    <P270>Account name</P270>
  </config>
</gs_provision>
```

示例文件中的 mac 要素是非必须要素，这样设计的原因是并非所有的自动配置系统都支持 MAC

地址。如果配置文件中出现 mac 要素，则自动配置程序会用此要素的值与话机的实际 MAC 地址进行对比验证。

XML 文件加密

XML 配置文件可以使用 AES-256-CBC 算法进行加密。加密技术的密码在 XML 配置文件中的 P1359 要素（XML 配置文件密码）中定义。此加密技术可以使用 Salt 散列提高安全性。从密码中获得密钥和 IV 的算法与 OpenSSL 使用的算法相同。

OpenSSL 中用于加密文件的命令行如下：Openssl enc –e –aes-256-cbc –k password –in config.xml –out cfgxxxxxxxxxxxx.xml

另外，用户也可以通过设备内嵌的 Web 页面设置 XML 配置文件的密码。

图2. 通过 Web 页面设置 XML 配置文件密码

当 XML 配置文件使用 AES-256-CBC 算法加密后，只有用户在 Web 界面或者二进制配置文件的 P1349 要素中设置了 XML 配置文件的密码后，设备才能解析此配置文件。

自动配置的安全性

尽管 XML 配置文件经过加密，并且其使用的加密算法——256-bit 密钥长度的 AES 算法——被认为是安全而强大的，但是也会导致一个问题：如何解析和加载初始的 XML 加密密码？解决此问题的方法有以下几种：

1. 使用原有的二进制配置文件设置初始的 XML 加密密码。此二进制配置文件是加密的并且普遍认为是安全的。
2. 使用 HTTPS 和客户端鉴权。这种方法符合工业标准，并且具有最强的安全性。