设置

设置概述

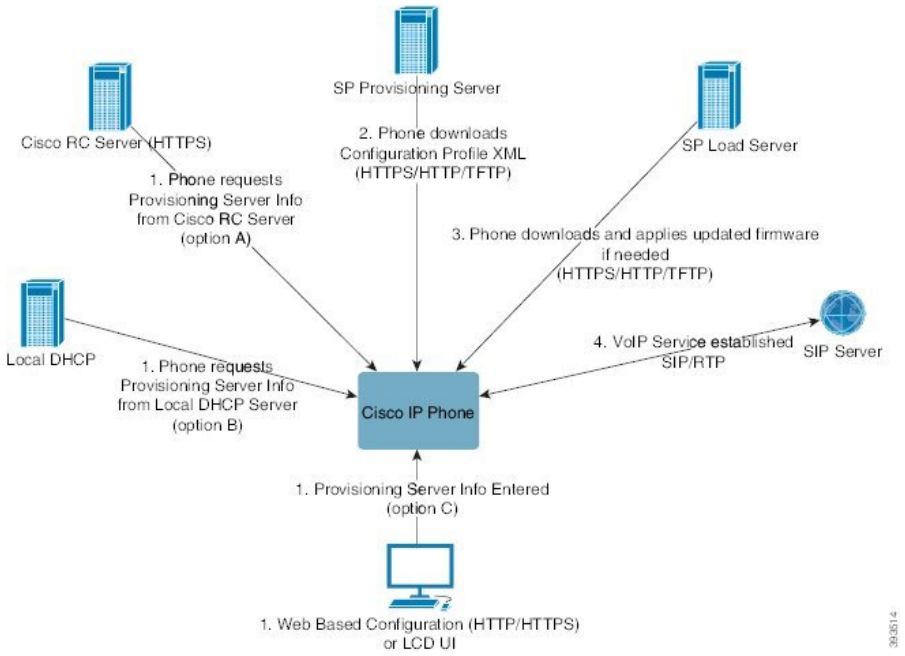
Cisco IP 电话主要供 IP 语音 (VoIP) 服务提供商为家庭、商务或企业环境中的客户大批量部署。 因此，通过远程管理和配置设置电话可确保在客户现场正确操作电话。

思科支持通过以下方式持续对电话进行自定义功能配置：

- 可靠地远程控制电话。
- 对控制电话的通信加密。
- 简化电话帐户绑定。

电话可设置为从远程服务器下载配置文件或更新的固件。 下载可能在三种情况下发生：电话连接到网络、电话接通电源，以及在设定的时间间隔。 设置通常是服务提供商经常执行的大批量 VoIP 部署的一部分。 配置文件或更新的固件将使用 TFTP、HTTP 或 HTTPS 传输到设备。

设置



简而言之，电话设置过程如下：

1. 如果电话未配置，设置服务器信息将使用以下选项之一应用到电话：
   - **A** – 使用 HTTPS、DNS SRV、GDS（激活码加入）、EDOS 设备激活，从 Cisco 支持数据编排系统 (EDOS) 远程自定义 (RC) 服务器下载。
   - **B** - 从本地 DHCP 服务器查询。
   - **C** – 使用 Cisco 电话基于 web 的配置实用程序或电话 UI 手动输入。
2. 电话使用 HTTPS、HTTP 或 TFTP 协议下载设置服务器信息以及应用配置 XML。
3. 如果需要，电话将使用 HTTPS、HTTP 或 TFTP 下载并应用更新的固件。
4. 使用指定的配置和固件建立 VoIP 服务。

VoIP 服务提供商致力于为住宅和小型企业客户部署多部电话。 在商务或企业环境中，电话可用作终端节点。 提供商在 Internet 上广泛分发这些设备，它们通过客户场所的路由器和防火墙连接。

电话可以用作服务提供商后端设备的远程分机。 远程管理和配置可确保在客户场所正确操作电话。

设置

可以配置电话，使其定期以及在接通电源时重新同步其内部配置状态，以便与远程配置文件匹配。 电话将联系一般设置服务器 (NPS) 或访问控制服务器 (ACS)。

默认情况下，只会在电话处于空闲状态时尝试配置文件重新同步。 这种做法可防止将触发软件重启以及中断呼叫的升级。 如果必须进行中间升级才能从旧版本升级到当前升级状态，升级逻辑可以自动执行多级升级。

一般设置服务器

一般设置服务器 (NPS) 可以是 TFTP、HTTP 或 HTTPS 服务器。 可以使用 TFTP、HTTP 或 HTTPS 远程完成固件升级，因为固件中不包含敏感信息。

尽管我们建议使用HTTPS，但与NPS的通信并不要求一定使用安全协议，因为更新的配置文件可用共享密钥加密。 有关使用 HTTPS 的详细信息，请参阅通信加密，第 11 页。 安全的首次设置通过使用 SSL 功能的机制完成。 未设置的电话可以接收以该设备为目标的 256 位对称密钥加密配置文件。

电话设置实践

通常情况下，Cisco IP 电话会在首次连接到网络时配置以进行设置。 服务提供商或 VAR 预设置（配置）电话时，也会在预定的时间间隔设置电话。 服务提供商可以使用电话键盘授权 VAR 或高级用户手动设置电话。 您还可以使用电话的 Web UI 配置设置。

从电话的 LCD UI 选择**状态** > **电话状态** > **设置**，或者在基于 web 的配置实用程序的**状态**选项卡上选择“设置状态”。

使用激活码加入您的电话

11-2-3MSR1 版固件、BroadWorks 应用程序服务器版本 22.0（修补程序 AP.as 22.0.1123 ap368163 及其依赖项）中提供了此功能。不过，您可以用较旧的固件改装电话以使用此功能。您可以指示电话升级到新固件，并使用 `gds://` 配置文件规则触发激活码屏幕。 用户在提供的字段中输入一个 16 位的代码以自动自行加入电话。

开始之前

确保允许 activation.Webex.com 服务通过防火墙，以支持通过激活码加入。

如果要为激活设置代理服务器，请确保正确配置了代理服务器。 请参阅：设置代理服务器。

过程

步骤 1 在文本编辑器或 XML 编辑器中编辑电话 config.xml 文件。

步骤 2 按照 config.xml 文件中的以下示例设置激活码加入的配置文件规则。

```
<?xml version="1.0" encoding="UTF-8"?>
<device>
<flat-profile>
<!-- System Configuration -->
<Profile_Rule ua="na">gds://</Profile_Rule>
<!--  Firmware Upgrade  -->
<Upgrade_Enable ua="na">Yes</Upgrade_Enable>
<Upgrade_Error_Retry_Delay ua="na">3600</Upgrade_Error_Retry_Delay>
<Upgrade_Rule ua="na">http://<server ip address>/sip88xx.11-2-3MSR1-1.loads</Upgrade_Rule>
<!-- <BACKUP_ACS_Password ua="na"/> -->
</flat-profile>
</device>
```

注释　对于 11.2 (3) SR1 之后的固件版本，固件升级的设置是可选的。

步骤 3 保存对 config.xml 文件的更改。

通过 CDA 重试加入设备

为配置电话以进行设置，通过 DHCP 选项、DNS SRV、CDA 设备激活或激活代码加入对电话应用了设置服务器信息。 从固件版本 12.0 (3) 开始，为了简化设备加入体验并增强故障抵御能力，引入了使用 CDA 重试设置机制。 在此过程中，电话会呈现激活代码屏幕，或者电话会显示空屏幕。 重试过程在后端继续，但用户并不知道。 如果您错过了最初将电话 MAC 地址添加到 CDA 服务中，并且稍后在电话首次未能从 CDA 服务获取任何配置时添加了 MAC 地址，那么这有助于您远程设置电话。 在固件版本 12.0 (3) 中，借助重试机制，电话将使用指数回退计时器再次尝试 CDA。 用户还可以选择性地重新启动电话，使其在 CDA 服务上添加 MAC 地址后重试 CDA。

此设置在以下情况下进行：

- 当电话首次开箱并预装固件版本 12.0.3 或更高版本时。
- 当电话在运行固件版本 12.0.3 或更高版本期间恢复出厂设置时。

当发生 CDA 重试时，用户可以看到以下自定义状态变化：

- 自定义状态从 **GDS 挂起**更改为**挂起**。
- 自定义状态从**自定义挂起**更改为**挂起**。

如果远程自定义过程进入最终状态，并且自定义状态设置为**已中止**、**已获得**或 **GDS 已获取**，则 CDA 重试将停止。

注释　我们建议在开箱即用情况下保持 **Resync_Error_Retry_Delay** 值不变。 此外，该值必须始终等于或大于 60 秒。

电话加入 Webex 云

电话加入提供了一种简单且安全的方式，可将支持 Webex 的电话加入 Webex 云。 可以使用激活码加入 (GDS) 或电话 MAC 地址（EDOS 设备激活）来完成加入流程。

有关如何生成激活码的详细信息，请参阅《*Cisco* 多平台电话 *Cisco BroadWorks* 合作伙伴配置指南》。

有关支持 Webex 的电话加入的详细信息，请参阅《*Webex for Cisco BroadWorks* 解决方案指南》。

允许电话加入 Webex 云

将电话成功注册到 Webex 云后，电话屏幕上会显示一个云符号 。

开始之前

访问电话管理网页。 请参阅：访问电话 Web 界面。

过程

步骤 1 选择**语音** > **电话**。

步骤 2 在 **Webex** 部分，将 **Onboard Enable** 参数设置为 **Yes**。

您可以通过输入以下格式的字符串，在电话配置 XML 文件 (cfg.xml) 中配置此参数：

```
<Webex_Onboard_Enable ua="na">Yes</Webex_Onboard_Enable>
```

默认值：Yes

步骤 3 单击 **Submit All Changes**。

使用短激活码启用自动设置

遵循以下步骤通过简短的激活码启用自动设置。

开始之前

确保您的电话已使用固件版本 11.3(1) 或更高版本更新。

如果要为电话设置代理服务器，请确保正确配置了代理服务器。 请参阅：设置代理服务器。

查看如何为重定向配置文件设置 CDA 服务器：

https://community.cisco.com/t5/collaboration-voice-and-video/cisco-multi-platform-phones-cloud-provisioning-process/ta-p/3910244

过程

步骤 1 创建一个由 3 到 16 个字符（含）组成的重定向配置文件名称。 稍后将成为激活码。 使用以下格式之一：

- **nnn**.
- **nnnnnnnnnnnnnnnn**
- 3 到 16（含）个数字。 例如，**123456**

步骤 2 将您在步骤 1 中创建的配置文件名称提供给客户设备激活 (CDA) 支持团队，邮箱为 cdap-support@cisco.com。

步骤 3 请 CDA 支持团队启用您的配置文件以供发现。

步骤 4 当您从 CDA 支持团队收到确认时，将激活码分发给用户。

步骤 5 指示用户在激活屏幕上输入数字之前按井号 (#)。

从键盘手动设置电话

过程

步骤 1 按**设置**。

步骤 2 选择**设备管理** > **配置文件规则**。

步骤 3 使用以下格式输入配置文件规则：

```
protocol://server[:port]/profile_pathname
```

例如：

```
tftp://192.168.1.5/CP_x8xx_MPP.cfg
```

若未指定任何协议，系统会假设您指定了 TFTP。 如果未指定服务器名称，则使用请求 URL 的主机作为服务器名称。如果未指定端口，则使用默认端口（TFTP 为 69，HTTP 为 80，HTTPS 为 443）。

步骤 4 按**重新同步**。

适用于 HTTP 设置的 DNS SRV

适用于 HTTP 设置的 DNS SRV 功能支持自动设置多平台电话。 域名系统服务 (DNS SRV) 记录在服务和主机名之间建立连接。 当电话查找设置服务的位置时，首先查询给定的 DNS SRV 域名，然后查询 SRV 记录。 电话验证记录以确认服务器可访问。 然后，它继续进行实际的设置流。 服务提供商可以利用此 DNS SRV 设置流来提供自动设置。

DNS SRV 基于 DHCP 提供的域名证书进行主机名验证。所有 SRV 记录一定要使用包含 DHCP 提供的域名的有效证书。

DNS SRV 查询包括其构造中的 DHCP 域名，如下所示：
<servicename>.<transport>.<domainName>。

例如，**_ciscoprov-https._tls.example.com**，指示电话对 example.com 执行查找。 电话使用 DNS SRV 查询检索到的主机名和端口号构建用于下载初始配置的 URL。

DNS SRV 是电话使用的许多自动设置机制之一。 电话将按以下顺序尝试这些机制：

1. DHCP
2. DNS SRV
3. EDOS
4. GDS（激活码加入）或 EDOS 设备激活

下表说明了 SRV 记录字段。

表 *1: SRV* 记录字段

字段	说明	示例
<_servicename.>	服务名称以下划线开头。 服务器服务在 SRV 记录中使用符号名称。 服务后的点号(.)表示服务已建立，下一部分开始。	**_ciscoprov-https.** 或 **_ciscoprov-http.** DNS SRV 不支持 TFTP 协议。如果您使用 TFTP，将会收到以下错误消息：错误 - SRV 查找中不支持 TFTP 方案。
<_proto.>	传输协议以下划线开头。 协议后的点号表示协议部分已结束。	**_tls.**您必须对 TLS 使用 HTTPS。 或者 **_tcp.**您必须对 TCP 使用 HTTP。
<domainName>	服务域名遵循协议。 主机名验证：所有 SRV 记录都根据最初 DHCP 提供的域名进行验证。所有记录一定要使用包含原始域名的有效证书。	**example.com**
TTL（存活时间）	记录的到期值（以秒为单位）。	86400
等级	互联网类型 — 标准 BIND 符号，表示它是 SRV 记录。	IN
<priority>	每条线路都包含一个优先级号码。 号码越小，电话将越早尝试包含在此 DNS SRV 记录中的目标主机名和端口。	**10**
<weight>	如果两个或多个服务具有相同的优先级，则权重号会确定哪条线路先到达。 号码越小，电话将越早尝试包含在此 DNS SRV 记录中的目标主机名和端口。	**20**
<port>	可选端口号	**5060**
<target>	提供服务的计算机的 A 记录。 记录是最基本的 DNS 记录类型，用于将域或子域指向 IP 地址。	**pr1.example.com**

SRV 配置示例

_service._proto.name. TTL class SRV priority weight port target.

_ciscoprov-https._tls.example.com. 86400 IN SRV 10 60 5060 pr1.example.com.

_ciscoprov-https._tls.example.com. 86400 IN SRV 10 20 5060 pr2.example.com.

_ciscoprov-http._tcp.example.com. 86400 IN SRV 10 50 5060 px1.example.com.

_ciscoprov-http._tcp.example.com. 86400 IN SRV 10 30 5060 px2.example.com.

使用适用于 HTTP 设置的 DNS SRV

新电话将 DNS SRV 用作自动设置的方法之一。 对于现有电话，如果您的网络设置为使用 HTTP 的 DNS SRV 设置，则可以使用此功能重新同步电话。 配置文件示例：

```
<flat-profile>
<!-- System Configuration -->
<Primary_DNS ua="rw">10.89.68.150</Primary_DNS>
<Back_Light_Timer ua="rw">Always On</Back_Light_Timer>
<Peer_Firmware_Sharing ua="na">Yes</Peer_Firmware_Sharing>
<Profile_Authentication_Type ua="na">Basic Http Authentication </Profile_Authentication_Type>
<Proxy_1_ ua="na">example.com</Proxy_1_>
<Display_Name_1_ ua="na">4081001141</Display_Name_1_>
<User_ID_1_ ua="na">4081001141</User_ID_1_>
</flat-profile>
```

开始之前

如果要为 HTTP 配置设置代理服务器，请确保正确配置了代理服务器。 请参阅：设置代理服务器。

过程

执行以下操作之一。 然后，使用 Web 页面上的 SRV 选项设置配置文件规则，第 8 页或在电话上通过 SRV 选项设置配置文件规则，第 9 页

- 将 XML 配置文件 ($PSN.xml) 放在 Web 服务器根目录中。
- 将 XML 配置文件 ($MA.cfg) 放在 Web 服务器根目录/Cisco/。

使用 Web 页面上的 SRV 选项设置配置文件规则

您可以使用 SRV 选项将配置文件下载到您的电话。

开始之前

访问电话 Web 界面

过程

步骤 1 选择 **语音** > **设置**

步骤 2 在 **Profile Rule** 字段中，通过 SRV 选项输入配置文件规则。 仅支持 HTTP 和 HTTPS。

示例：

```
[--srv] https://example.com/$PSN.xml
```

在电话上通过 SRV 选项设置配置文件规则

您可以使用电话上的 SRV 选项下载配置文件。

过程

步骤 1 按**设置**。

步骤 2 选择**设备管理** > **配置文件规则**。

步骤 3 使用 **[--srv]** 参数输入配置文件规则。 仅支持 HTTP 和 HTTPS。

示例：

```
[--srv] https://example.com/$PSN.xml
```

步骤 4 按**重新同步**。

TR69 设置

Cisco IP 电话可帮助管理员使用 Web UI 配置 TR69 参数。 如需参数相关信息，包括 XML 和 TR69 参数的比较信息，请参阅相应电话系列的管理指南。

电话支持自 DHCP 选项 43、60 和 125 的自动配置服务器 (ACS) 发现。

- 选项 43 – ACS URL 的供应商特定信息。
- 选项 60 – 供应商类别标识符，适用于向 ACS 将自身标识为 `dslforum.org` 的电话。
- 选项 125 – 网关关联的供应商特定信息。

TR69 RPC Methods

支持的 RPC 方法

电话仅支持一组有限的远程过程调用 (RPC) 方法，如下所示：

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- GetParameterNames
- AddObject
- DeleteObject
- Reboot
- FactoryReset
- Inform
- Download：下载 RPC 方法，受支持的文件类型包括：
  - 固件升级图像
  - 供应商配置文件
  - 自定义证书权限 (CA) 文件
- Transfer Complete

支持的事件类型

电话支持基于受支持功能和方法的事件类型。 仅支持以下事件类型：

- Bootstrap
- Boot
- value change
- connection request
- Periodic
- Transfer Complete
- M Download
- M Reboot

通信加密

传送给设备的配置参数可能包含阻止系统遭未经授权访问的授权码或其他信息。 防止未经授权的客户活动符合服务提供商的利益。 防止帐户遭未经授权使用符合客户的利益。 除限制对管理 web 服务器的访问权限之外，服务提供商可以对设置服务器与设备之间的配置文件通信加密。

网络拥塞期间的电话行为

任何降低网络性能的因素都会影响电话音频质量，且在某些情况下，会导致呼叫掉线。 造成网络性能降低的原因包括但不限于以下活动：

- 管理工作，例如内部端口扫描和安全性扫描。
- 您的网络上发生的攻击，例如阻断服务攻击。

内部预设置和设置服务器

服务提供商会通过配置文件预设置电话，而非远程自定义设备。 预设置配置文件中可能包含一组重新同步电话的有限参数。配置文件也可包含远程服务器交付的一整组参数。默认情况下，电话会在接通电源时以及按照配置文件中配置的间隔重新同步。 当用户在客户场所连接电话时，设备会下载更新的配置文件以及任何固件更新。

可以通过多种方法完成这一预设置、部署和远程设置的流程。

服务器准备和软件工具

本章中的示例要求一个或多个服务器可用。 这些服务器可以安装在本地 PC 上，并在其上运行：

- TFTP（UDP 端口 69）
- 系统日志（UDP 端口 514）
- HTTP（TCP 端口 80）
- HTTPS（TCP 端口 443）。

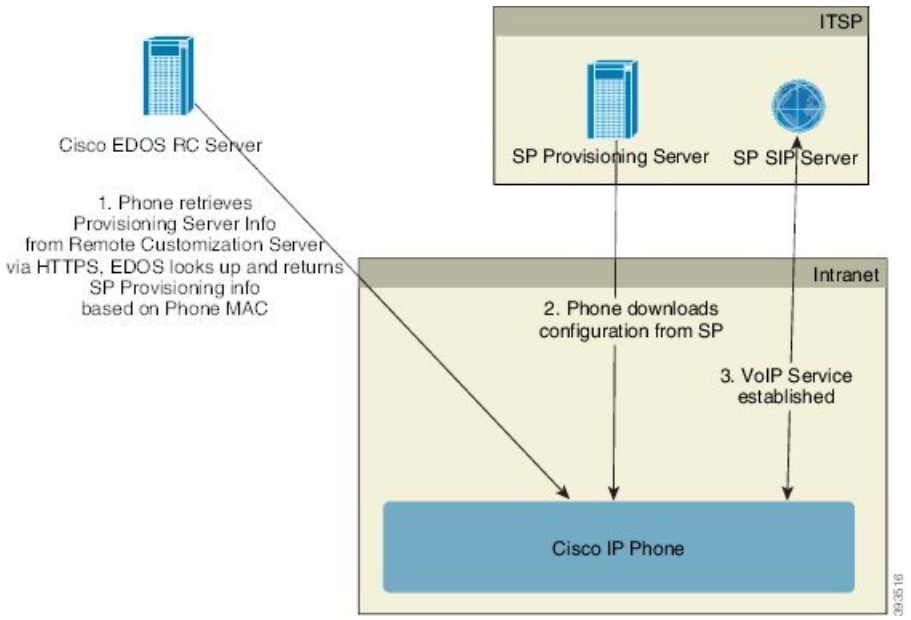
要对服务器配置进行故障排除，最好在单独的服务器机器上安装每类服务器的客户端。 这种做法可以建立适当的服务器操作，而不受与电话交互的影响。

我们还建议您安装以下软件工具：

- 要生成配置文件，安装开放源码 gzip 压缩实用程序。
- 对于配置文件加密和 HTTPS 操作，安装开放源码 OpenSSL 软件包。

- 要使用 HTTPS 测试动态配置文件生成和单步远程设置，我们推荐使用支持 CGI 脚本的脚本语言。 开放源码 Perl 语言工具就是这种脚本语言的一个例子。
- 要验证设置服务器与电话之间的安全交换，请安装以太网数据包探查器（如可免费下载的 Ethereal/Wireshark）。 捕获电话与设置服务器之间的以太网数据包交互跟踪记录。 为此，请在连接至启用了端口镜像的交换机的 PC 上运行数据包嗅探器。 对于 HTTPS 事务，您可以使用 ssldump 实用程序。

远程自定义 (RC) 分配



在初次设置之前，所有电话都会联系 Cisco EDOS RC 服务器。

在 RC 分配模式下，客户购买已与 Cisco EDOS RC 服务器中的特定服务提供商关联的电话。 Internet 电话服务提供商 (ITSP) 设置和维护设置服务器，并向 Cisco EDOS RC 服务器注册设置服务器信息。

当电话通过 Internet 连接供电时，未设置电话的自定义状态是**打开**。 首先，电话会向本地 DHCP 服务器查询设置服务器的信息，并设置电话的自定义状态。 如果 DHCP 查询成功，自定义状态将设置为**中断**，且不会因 DHCP 提供所需的设置服务器信息而尝试 RC。

电话第一次连接到网络时或恢复出厂设置后，如果没有设置 DHCP 选项，电话会联系设备激活服务器以执行零接触配置。 新电话将使用 “activate.cisco.com” 而不是 “webapps.cisco.com” 进行配置。 如果固件版本为 11.2 (1)，电话将继续使用 webapps.cisco.com。 思科建议您允许这两个域名通过防火墙。

如果 DHCP 服务器不提供设置服务器信息，电话会查询 Cisco EDOS RC 服务器，并提供其 MAC 地址和模型，自定义状态将设置为**挂起**。 Cisco EDOS 服务器响应关联服务提供商的设置服务器信息，包括设置服务器 URL，电话的自定义状态将设置为**自定义挂起**。 电话随后会执行重新同步 URL 命令，以检索服务提供商的配置，如果成功，自定义状态将设置为**已获得**。

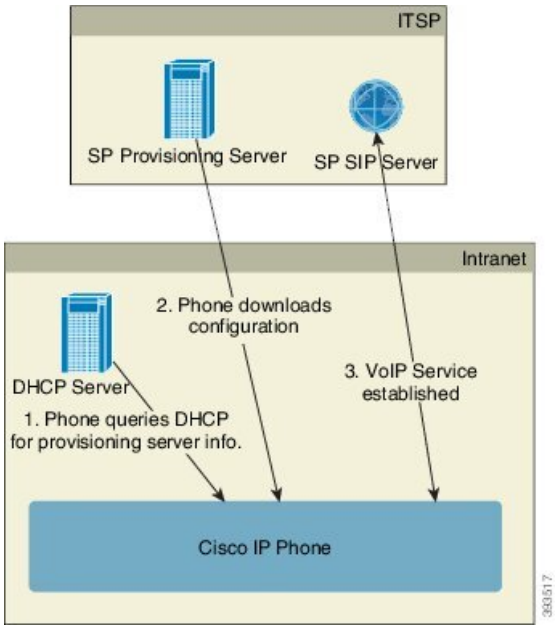
如果 DHCP 服务器设置失败，电话会查询 Cisco EDOS RC 服务器，并提供其 MAC 地址和模型，自定义状态将设置为**挂起**。 Cisco EDOS 服务器响应关联服务提供商的设置服务器信息，包括设置服务器 URL，电话的自定义状态将设置为**自定义挂起**。 电话随后会执行重新同步 URL 命令，以检索服务提供商的配置，如果成功，自定义状态将设置为**已获得**。 如果用于本地 DHCP 服务器或 EDOS 服务器的查询因配置而失败，电话将重试以在 DHCP 和 EDOS 上自行激活。

如果 Cisco EDOS RC 服务器没有与电话关联的服务提供商，电话的自定义状态将设置为**不可用**。 可以手动配置电话，也可以为电话的服务提供商添加与 Cisco EDOS 服务器的关联。

如果电话通过 LCD 或 Web 配置实用程序设置，在自定义状态变为**已获得**之前，自定义状态将设置为**中断**，除非电话恢复出厂设置，否则 Cisco EDOS 服务器不会查询。

设置电话后，除非电话恢复出厂设置，否则不会使用 Cisco EDOS RC 服务器。

内部设备预设置



使用 Cisco 出厂默认配置，电话会自动尝试重新同步到 TFTP 服务器上的配置文件。 LAN 上的受管 DHCP 服务器提供与配置用于预设置到设备的配置文件和 TFTP 服务器相关的信息。 服务提供商将各部新电话连接到 LAN。 电话自动重新同步到本地 TFTP 服务器并初始化其内部状态，以便为部署做好准备。 此预设置配置文件通常包括远程设置服务器的 URL。 当设备部署完毕并连接到客户网络后，设置服务器会保持设备更新。

电话发送给客户前，可以扫描预设置设备的条形码，以记录其 MAC 地址或序列号。 此信息可用于创建电话将重新同步的配置文件。

收到电话之后，客户会将其连接到宽带链路。 开机时，电话将利用通过预设置配置的 URL 联系设置服务器。 因此，电话将根据需要重新同步和更新配置文件及固件。

设置服务器的设定

本节介绍使用各种服务器和不同场景设置电话的设定要求。 出于本文档和测试的目的，设置服务器安装在本地 PC 上并在其上运行。 而且，通用软件工具对于设置电话很有用。

TFTP 设置

电话支持 TFTP 用于设置重新同步和固件升级操作。 如果设备是远程部署，建议使用 HTTPS，不过也可以使用 HTTP 和 TFTP。 这就需要设置文件加密以增强安全性，因为它采用 NAT 和路由器保护机制，提供了更高的可靠性。 TFTP 对于内部预设置大量未设置的设备非常有用。

电话能够通过 DHCP 选项 66 直接从 DHCP 服务器获得 TFTP 服务器 IP 地址。如果配置 profile _ rule 与该 TFTP 服务器的 filepath 一起配置，则设备将从 TFTP 服务器下载其配置文件。 当设备连接到 LAN 并接通电源时，即会开始下载。

对于具有出厂默认配置文件的设备，在接通电源时，设备将重新同步到 DHCP 选项 66 指定的本地 TFTP 服务器上的此文件。 文件路径与 TFTP 服务器虚拟根目录相关。

远程终端控制和 NAT

电话与网络地址转换 (NAT) 兼容，从而通过路由器访问 Internet。 为增强安全性，路由器可能会尝试通过实施对称 NAT 来阻止未经授权的传入数据包，这是一种严格限制可从 Internet 进入受保护网络的数据包过滤策略。 为此，不建议使用 TFTP 进行远程设置。

仅当提供某种形式的 NAT 穿越时，VoIP 才可与 NAT 共存。 配置通过 NAT 的简单 UDP 穿越 (STUN)。此选项要求用户具备：

- 来自您服务的动态外部（公共）IP 地址
- 运行 STUN 服务器软件的计算机
- 具有非对称 NAT 机制的边缘设备

HTTP 设置

电话的行为方式与从远程 Internet 站点请求网页的浏览器类似。 这将提供到达设置服务器的可靠方式，即使客户路由器实施对称 NAT 或其他保护机制亦不受影响。 在远程部署中，HTTP 和 HTTPS 比 TFTP 可靠，特别是当部署的设备在居民防火墙或支持 NAT 的路由器后面连接时。 在下列请求类型说明中，HTTP 和 HTTPs 可以互换使用。

基于基本 HTTP 的设置依赖于 HTTP GET 方法来检索配置文件。 通常，会为所部署的每部电话创建一个配置文件，这些文件存储在 HTTP 服务器目录中。 当服务器收到 GET 请求时，其仅返回 GET 请求标头中指定的文件。

配置文件可以通过查询客户数据库并实时生成配置文件来动态生成，而非静态。

当电话请求重新同步时，它可以使用 HTTP POST 方法请求重新同步配置数据。 可以配置设备，在 HTTP POST 请求的正文内向服务器传达特定状态和标识信息。 服务器使用此信息生成所需的响应配置文件，或存储状态信息供日后分析和跟踪。

作为 GET 和 POST 请求的一部分，电话会自动在请求标头的“用户-代理”字段中包含基本标识信息。 此信息包括制造商、产品名称、当前固件版本和设备的产品序列号。

下面的示例是来自 CP-7832-3PCC 的“用户-代理”请求字段：

```
User-Agent: Cisco-CP-7832-3PCC/11.0.1 (00562b043615)
```

用户代理是可配置的，如果尚未配置，电话将使用此值（仍然是默认值）。

将电话配置为使用 HTTP 重新同步到配置文件时，建议使用 HTTPS 或对配置文件加密以保护机密信息。 电话通过 HTTP 下载的加密配置文件避免了暴露配置文件中包含的机密信息的危险。 相比使用 HTTPS，这种重新同步模式在设置服务器上产生的计算负载较少。

电话可解密使用以下加密方法之一加密的配置文件：

- AES-256-CBC 加密
- 使用 AES-128-GCM 加密算法的基于 RFC-8188 的加密

注释 当 HTTP 1.1 版是协商的传输协议时，电话支持 HTTP 1.0 版、HTTP 1.1 版和分块编码。

重新同步和升级时的 HTTP 状态代码处理

电话支持远程设置（重新同步）的 HTTP 响应。 当前电话行为以三种方式归类：

- A — 成功，其中“重新同步周期”和“重新同步随机延迟”值决定后续请求。
- B — 故障，找不到文件或者配置文件受损。 “重新同步错误重试延迟”值决定后续请求。
- C — 其他故障，URL 或 IP 地址不正确导致连接错误。 “重新同步错误重试延迟”值决定后续请求。

表 *2:* 针对 *HTTP* 响应的电话行为

HTTP 状态代码	说明	电话行为
301 Moved Permanently	此请求以及未来请求应定向到新的位置。	立即用新位置重试请求。
302 Found	被称为暂时移动。	立即用新位置重试请求。
3xx	不处理其他 3xx 响应。	C
400 Bad Request	由于语法不正确，不能满足请求。	C

HTTP 状态代码	说明	电话行为
401 Unauthorized	基本或 digest 访问验证质询。	立即用验证凭证重试请求。 最多重试 2 次。 发生故障时，电话行为是 C。
403 Forbidden	服务器拒绝响应。	C
404 Not Found	找不到请求的资源。 允许客户端的后续请求。	B
407 Proxy Authentication Required	基本或 digest 访问验证质询。	立即用验证凭证重试请求。 最多重试两次。 发生故障时，电话行为是 C。
4xx	不会处理其他客户端错误状态代码。	C
500 Internal Server Error	一般错误消息。	电话行为是 C。
501 Not Implemented	服务器不识别请求方法，或无法完成请求。	电话行为是 C。
502 Bad Gateway	服务器充当网关或代理，接收来自上游服务器的无效响应。	电话行为是 C。
503 Service Unavailable	服务器当前不可用（过载，或因维护而停机）。 这是一个临时状态。	电话行为是 C。
504 Gateway Timeout	服务器充当网关或代理，不接收来自上游服务器的及时响应。	C
5xx	其他服务器错误	C

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。