

6.2 密码恢复案例

随着因特网规模的不断扩大,网络与我们的生活已经越来越近,许多政府、学校和公司都组建了自己的信息网络,这使得交换机和路由器这一网络设备的使用越来越广泛。在使用交换机和路由器的过程中经常会出现忘记密码的事情,使维护人员无法登录,影响工作的进一步开展。本节将介绍恢复交换机密码的思路和步骤。

6.2.1 案例场景描述

众所周知,交换机和路由器都需要有一定的安全保证,也就是说,要及时为它们配置合理的密码,那么,如果这个密码忘记了怎么办呢?

某公司的网络管理员离职,新招聘的网络管理员准备重新配置交换机的一些参数。但发现其中多台交换机的密码与“密码本”的记录不一致。公司所有的网络设备大致有3个密码,很多人都帮助猜测这个密码,分别尝试了“原网络管理员的生日”和一些默认密码,但都无法登录,如图6-2所示。

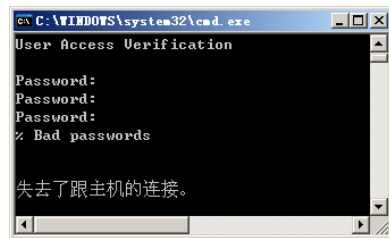


图 6-2 交换机登录密码错误

6.2.2 解决思路

以这家公司网络管理的情况来看,极有可能是没有交换机和路由器运行配置文件的备份,因此需要在不破坏交换机配置文件的情况下更改,并配置一个新的口令。

另外,这家公司所用的网络设备品牌很多,华为、实达和思科三分天下。首先要清楚一点,不同品牌的网络设备都自己拥有不同的文件系统,因此破解密码的方式也是不同的,下面以思科产品为例进行说明。



<http://www.cisco.com/warp/public/474/index.shtml> 提供了思科系列产品的口令恢复 (Password Recovery Procedures) 手册。

或者访问国内网站 http://www.net130.com/cms/Pubpspecial/special_password/202320.htm 部分 CISCO 密码恢复手册。

1. 密码恢复原理

所有的 Cisco 路由器都具有一个位于 NVRAM 中的 16 位软件寄存器。默认情况下,配置寄存器设置是从闪存加载 Cisco IOS,并且从 NVRAM 查找并加载 startup-config 文件。在动手恢复密码之前,首先要进一步了解 IOS 的特性管理。

1) 操作系统模式

路由器可以加载 3 种类型的操作系统:

(1) 全功能的 IOS

一般在闪存中,可以放在 TFTP 服务器中;应用于产品的全功能的普通 IOS。

(2) 限制功能的 IOS

一般在 ROM 中具备基本的 IP 连通性,用于闪存出现故障而用户需要通过 IP 连接来复制一份新的 IOS 到闪存中的情况,称为 RXBOOT 模式。

(3) ROM Monitor

通常用于 Cisco TAC 的低级调试及口令恢复,称为 ROM Monitor 模式。



对于许多初学者来说，不建议使用 Cisco 路由器的 ROM Monitor 模式。原因很简单：一是我们并不经常用到该模式，对其相关操作不熟悉；二是在 ROM Monitor 模式下的操作失误，往往会对路由器造成致命的伤害（比如破坏 Flash 中的 IOS 文件，导致系统崩溃）。

2) IOS 启动顺序

IOS 软件包的启动顺序如下所述，大致分为 4 步。

第 1 步：路由器执行加电自检（POST）以查找和验证硬件。

第 2 步：路由器从 ROM 中加载并运行自引导程序代码。

第 3 步：路由器加载 IOS 或其他软件。

第 4 步：路由器找到配置文件并将它加载到运行配置中。

具体的启动顺序可能还要复杂一些，如图 6-3 所示。

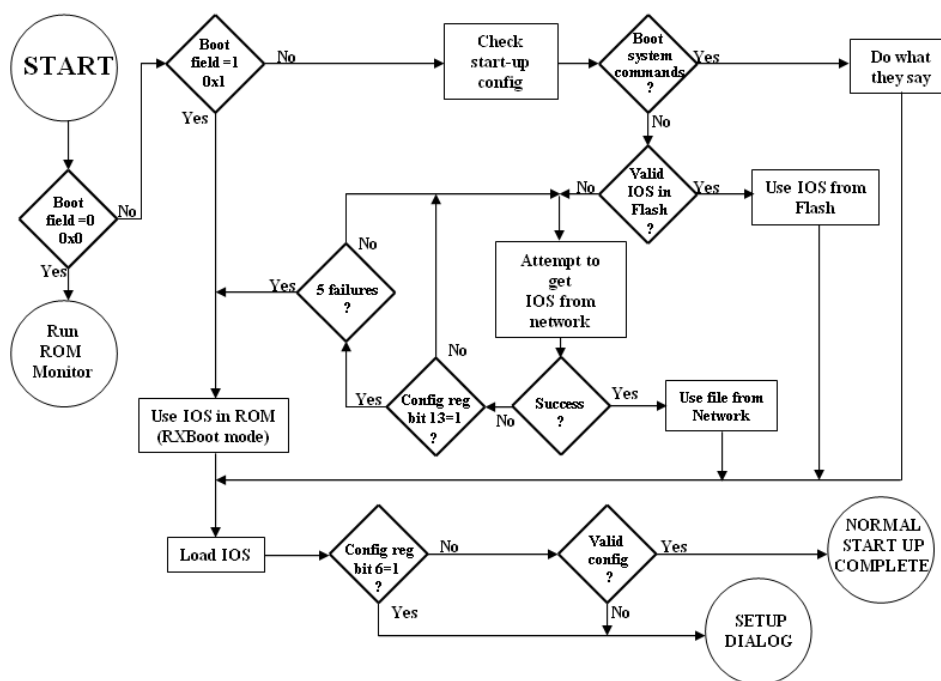


图 6-3 路由器启动流程图

路由器在每次加电或重新启动时都试图全部完成这 4 步。路由器管理员不能更改 POST 代码及其功能。注意在自引导程序代码的位置，要加载的 IOS 及配置文件是可以改变的，但是自引导程序代码和初始配置几乎总是放在它们默认的位置上，也就是说，自引导程序代码放在 ROM 里，而初始配置一般都放在 NVRAM 中。因此，IOS 或其他软件的位置就成了一般情况下唯一需要改动的部分。

3) 寄存器值得设定

下面讨论配置寄存器的设置及如何使用这些设置恢复路由器的口令。配置寄存器的 16 位从左到右依次为 15、14、13、……、0。Cisco 路由器默认的配置设置是 0x2102（0x 表示是十六进制）。也就是说，第 13 位、第 8 位和第 1 位的值是 1，如表 6-16 所示。

表 6-16 寄存器位

寄存器	2				1				0				2			
位值	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
二进制	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0

各软件配置位的意义如表 6-17 所示。注意第 6 位用于忽略 NVRAM 的内容。此位既可

用于口令恢复。

表 6-17 各软件配置位数值与解释

位	十六进制	解 释
0~3	0x0000~0x000f	启动字段（参见表 6-18）
6	0x0040	忽略 NVRAM 内容
7	0x0080	启用 OEM 位
8	0x0100	禁用中断
10	0x0400	IP 广播全为零
5,11~12	0x800~0x1000	控制台线路速率
13	0x2000	如果网络启动失效则启动默认 ROM 软件
14	0x4000	IP 广播不包含网络号
15	0x8000	启动诊断信息并忽略 NVRAM 内容

注意，位于配置寄存器 0~3 位的启动字段控制路由器的启动顺序，表 6-18 中进一步说明了各个位的用途。

表 6-18 启动字段及其用途

启动字段	意 义	用 途
00	ROM 监控模式	若要启动时采用 ROM 监控模式，将配置寄存器的值设置为 2100。必须用 b 命令来手动启动路由器。路由器将显示 rommon>作为提示
01	从 ROM 启动映像文件	若要启动存储在 ROM 中的 IOS 映像文件，将配置寄存器的值设置为 2101。路由器将显示 router (boot) >作为提示
02~F	指定默认启动文件名	任何从 2102~210F 的值将告诉路由器使用 NVRAM 中指定的启动命令

2. 路由器密码恢复

这里假设之前对路由器寄存器的值作了修改，使用 show version 命令，检查当前配置寄存器值，如图 6-4 所示：

最后一行的信息是配置寄存器的值，在这里是 0x2142，即下次启动时不加载 startup-config 文件，正常情况下的值应该是 0x2102。由此可见，只要中断路由器的启动过程，跳过 startup-config 中包含的密码验证，也就意味着密码将不在起作用了。

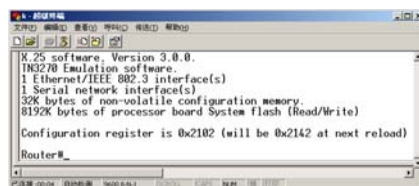


图 6-4 检查寄存器值

默认的配置寄存器的值是 0x2102，意味着第 6 位是关闭的（值为 0）。在默认情况下，路由器会查找并加载存储在 NVRAM 中的路由器配置文件（startup-config 文件）。若要恢复口令，需要开启配置寄存器的第 6 位，告诉路由器忽略 NVRAM 的内容。开启了第 6 位的配置寄存器值是 0x2142。

以下是口令恢复的主要步骤。

- 第 1 步：启动路由器并通过执行一个中断来中断启动顺序。
- 第 2 步：修改配置寄存器开启第 6 位（值为 0x2142）。
- 第 3 步：重载路由器。
- 第 4 步：进入特权模式。
- 第 5 步：将 startup-config 文件复制为 running-config 文件。
- 第 6 步：修改口令。
- 第 7 步：将配置寄存器重设为默认值。
- 第 8 步：保存配置。
- 第 9 步：重新加载路由器。

3. 交换机密码恢复

交换机口令恢复的原理类似于路由器，交换机恢复密码的过程主要是通过停止引导过程，不使用配置文件的方式来实现，但是具体的操作方法不同。CatOS 与 IOS 交换的密码恢复过程也是不同的，由于这家公司中存在着几个不同型号的 Cisco 设备，因此在后面的操作过程中要针对不同型号制订恢复策略。

6.2.3 密码恢复过程

由于远程破解这些设备的密码的机会很小，网管员放弃了这种想法，携带好串口电缆和笔记本来到机柜旁边，开始逐步破解各个设备的密码。

首先需要把串口电缆的一端插在网络设备背面的 Console 口中，另一端插在普通电脑的串口里。当交换机加电后，操作系统中使用“超级终端”程序。打开“超级终端”，在设定好连接参数后，就可以进行密码破解了。

1. Cisco 2500 和 2600 路由器

第 1 步：启动路由器并执行一个中断。

当路由器重新启动时，按下笔记本中的【Ctrl+Break】键，中断路由器启动，这时能看到一个提示符 Rommon 1>（这是 2600 系列的路由器提示）；而对于 2500 系列的路由器提示符是“>”。

第 2 步：修改配置寄存器。对于 2600 系列，命令是 Rommon 1>Config-register 0x2142；对于 2500 系列命令为>o/r 0x2142。

第 3 步：重载路由器并进入特权模式。

在 2600 系列上，输入 reset。在 2500 系列路由器上，输 I。路由器将重新加载，此时会询问是否要使用设置模式，回答 No，按回车进入用户模式，键入 Enable 命令，进入特权模式。

第 4 步：查看并修改配置。

现在需要将 startup-config 复制为 running-config 文件，让路由器此时运行的状态保持正常 copy startup-config running-config，此时配置正在 RAM 中运行，在特权模式下，可以修改配置。注意：此时虽然进入了路由器，但依然不能查看离职管理员，用 enable secret 设置的加密口令，只能修改成为一个新的密码把它修改，如下：

```
configure terminal
enable secret (password)
```

第 5 步：重设配置寄存器并重载路由器。

修改口令之后，一定要使用 config-register 将配置寄存器设置回默认值 Config-register 0x2102，最后保存配置 copy running-config startup-config 并重载路由器，口令恢复结束。



提示

一定要注意第 2 步和第 5 步中的命令，切不可颠倒顺序。由于输入失误，我们在一项工程实施中导致客户数据丢失，造成网络瘫痪多达 4 个小时的事故。

2. 在 COS 交换机上恢复口令

对于 CatOS 的 Catalyst 交换机，口令恢复步骤如下。

第 1 步：正确连接到交换机（硬件和软件）。

第 2 步：重新打开交换机在加电自检过程中操作。

第 3 步：在交换机开机的 30 秒内，按顺序完成下面的工作。

- 在口令提示符处按下回车键，输入一个空口令。
- 在提示符处输入 enable，进入特权模式。
- 在口令提示符处按下回车键，输入一个空口令。

- 使用 `set password` 命令或 `set enablepass` 命令改变口令。
- 在提示符处按下回车键来输入口令。

第 4 步：保存配置，完成。



由于需要管理员在 30 秒之内输入命令，为避免输入错误等操作影响，可以将上述命令复制到 TXT 文本文件中，在使用时粘贴在操作控制台界面上即可。

3. Cisco IOS 交换机口令恢复

Cisco IOS 交换机比 CatOS 交换机口令恢复，甚至比路由器的口令恢复都要复杂一些。

第 1 步：断开交换机电源线。

第 2 步：在重新连接电源线时，一直按住交换机的 **MODE** 按钮。可以在 1X 接口的 LCD 灯不再亮的 1 秒或 2 秒后松开 **MODE** 按钮。这时 **System** 指示灯一直闪烁，控制台出现如下信息。

```
The system has been interrupted prior to initializing the flash filesystem. The following commands will initialize the flash filesystem, and finish loading the operating system software:
```

```
flash_init
boot
```

第 3 步：输入 `flash_init`，初始化 flash 文件系统。

```
Switch: flash_init
Initializing Flash...
flashfs[0]: 86 files, 4 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 15998976
flashfs[0]: Bytes used: 6639616
flashfs[0]: Bytes available: 9359360
flashfs[0]: flashfs fsck took 15 seconds.
...done Initializing Flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
```

第 4 步：输入 `load_helper`，装载并初始化辅助映像（Helper Imager），这是存储在 ROM 中的迷你 IOS 映像，通常用灾难恢复。

第 5 步：输入 `dir flash:`（有冒号），显示 Flash 文件系统内的文件和目录列表。

```
Switch: dir flash:
Directory of flash:/
 2  -rwx  0      <date>          env_vars
 3  -rwx 344    <date>          system_env_vars
 4  -rwx  5      <date>          private-config.text
 6  -rwx 2149   <date>          config.text
 8  drwx 192    <date>          c3550-i9q3l2-mz.121-20.EA1a
9359360 bytes available (6639616 bytes used)
```

第 6 步：输入 `rename flash:config.text flash:config.old`，这个文件名可以自己确定，修改配置文件名。该文件包括了口令的设置。

第 7 步：输入 `boot`，重启系统。

第 8 步：重新启动后系统提示如下。

```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
Would you like to terminate autostall? [yes]: ✓
```

输入 `no`，不进入设置模式向导配置对话框。按 **【Enter】** 键进入用户模式。

第 9 步：在交换机的提示符下，输入 `enable` 进入特权模式。

第 10 步：输入 `rename flash:config.old flash:config.text`，将配置文件改回原来的默认名称。

第 11 步：将配置文件复制到 RAM 中，执行 `copy startup-config runnig-config`，现在配

置文件被加载。

第 12 步：修改口令。

第 13 步：保存配置。



在交换机 2950 上恢复口令时，第 2 步操作方法有点不同。开始也是一直按住面板上的 mode 按钮不放，插上交换机的电源线，注意观察面板，刚开始 stat 指示灯一直闪烁，system 指示灯亮，等 stat 指示灯灭掉，system 指示灯闪烁，此时放开 mode 按钮。控制台出现如下信息：

The system has been interrupted prior to initializing the flash filesystem. The following commands will initialize the flash filesystem, and finish loading the operating system software:

```
flash_init
load_helper
boot
```

然后在第 3 步中依次输入 flash_init 命令和 boot 命令，其他的操作步骤一致。

这家公司的路由器和 Cisco 3550、Cisco 3750 交换机都采用如下步骤破解了口令，并在修改密码后正常工作。采用本节介绍的方法，修改密码时不会把原来的配置文件内容清除掉，特别是一个生产网络里已经运行的交换机，这样比较保险。

6.3 操作系统备份与升级案例

基于安全的考虑，网络管理员要对网络设备的配置信息和 IOS 进行备份，如果需要将新的特性部署到网络设备上，很多时候就需要对 IOS 的版本进行升级。

不小心把 IOS 误删掉或者在升级 IOS 失败，重启后进入 ROMMON (ROMMON 状态是 ROM MONITOR 的缩写) 状态，是比较常见的事情。本节内容将介绍 IOS 备份与恢复的两种方法。

6.3.1 案例场景描述

很多想考 CISCO 认证的朋友经常苦于实战演练没有设备，北京某培训中心根据业务发展的情况，对部分 VIP 学员免费开放了实验环境。并且在这些设备所组成的拓扑上，配置和实现很多复杂的功能，但学员经常拔插 Console 线，这会对 Console 口造成极大的损伤。基于以上考虑，培训中心在原有培训实验室的基础上建立了一套远程试验室，大部分的实验环境都实现了隔离，也就是说，练习学员很少能接触到真实的设备。

实验室也进行了一些规定，例如一些危险性的命令 (erase flash) 是不允许操作的。但是还有一些学员并没有很好的遵守这些规定，导致一些设备出现了 IOS 损坏的情况。一些设备已经无法使用，只能进入 ROMMON 状态，不能进行正常的路由转发功能和软件配置，在这种模式下，原 IOS 中的大部分命令都无法使用。

网络管理员在修复这些设备时，首先检查了 config-register 设置的情况 (正常 config-register 应该是 0x2102 的)，但发现没有问题，已经可以确认是 IOS 遭到了致命的伤害。另外，一些网络设备的 IOS 版本特性已经升级了，在获取新的 IOS 后也需要对这些设备进行更新操作。培训中心的网络维护需求如下：

- 升级一些交换机的 IOS 版本，让交换机支持更多的特性。
- 修复被破坏的路由器 IOS。

**提示**

在实验环境中，升级 IOS 的情况也是比较常见的，例如，CISCO 2950 交换机频繁发生吊死故障，发生吊死的交换机无任何警告信息，重启后即恢复正常。通过将交换机 IOS 版本由 12.11 (EA1) 升级到 12.12(EA2) 之后的版本，故障现象就可以消失。

6.3.2 解决思路

在利用 config-register 检查寄存器没有问题的情况下，就需要检查 IOS 大小和文件名是否出现了改动。用 dir flash: 命令；注意命令中 flash 后面跟冒号“:”，执行命令后会显示 flash 现存的 IOS 大小和文件名，如下：

```
rommon 1 > dir flash:  
File size Checksum File name  
2179331 bytes (0x214103) 0x7b95 c1600-nsy-mz_112-15a_p
```

如果 File name 和 File size 的两项都和系统之前的快照不一致，那就需要操作系统恢复的步骤了。此时，管理员可以根据 IOS 的备份恢复系统，可以利用“TFTP”和“XMODEM”两种方式。下面介绍一下升级与备份前的准备工作。

1. 选择传输协议

升级或恢复 IOS 的方法可以有 3 种：TFTP、XMODEM 和 FTP，但前面两种比较常用。

在实验室升级网络设备的操作系统还是比较简单的，风险只存在实验网络，但在生产网络中升级 IOS 的风险是无处不在的。在高端设备的升级中，很有可能会发生一些意想不到的事，比如，用 TFTP 传输 Cisco 6509 交换机 IOS 就会出现这个问题，这是因为 TFTP (Trivial File Transfer Protocol) 普通文件传输协议最大就支持传输 32MB 的文件，而新的 IOS 要超过这个限制，所以需要使用 FTP 进行升级。

1) TFTP

TFTP (Trivial File Transfer Protocol, 简单文件传输协议) 是 TCP/IP 协议集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。TFTP 承载在 UDP 上，提供不可靠的数据流传输服务，不提供存取授权与认证机制，使用超时重传方式来保证数据的到达。

可以从它的名称上看出，它适合传送“简单”的文件。与 FTP 不同的是：它使用的是 UDP 的 69 接口，因此它可以穿越许多防火墙。不过它也有缺点，比如传送不可靠、没有密码验证等。虽然如此，它还是非常适合传送小型文件的，就比如网络设备的 IOS 文件。

2) XMODEM

XMODEM 协议是最早出现的两台计算机间通过 RS232 异步串口进行文件传输的通信协议标准，相对于 YMODEM、ZMODEM 等其他文件传送协议来说，XMODEM 协议实现简单，适合于那些存储器有限的场合。

XMODEM 文件发送方将文件分解成 128 字节的定长数据块，每发送一个数据块，等待对方应答后才发送下一个数据块，数据校验采用垂直累加和校验，也可以采用 16 位的 CRC 校验。属于简单 ARQ (自动请求重发) 协议，所以也适合于 2 线制的半双工的 RS485 网络中使用。

2. 升级准备与注意事项

操作系统作为一个复杂系统，不论在发布之前多么仔细地进行测试，总会有缺陷产生的。出现缺陷后的唯一办法就是尽快给系统打上补丁；如果是网络设备的操作系统，它与其他通用操作系统 (Windows 和 Linux) 的区别在于 IOS 需要将整个系统更换为打过补丁的系统。IOS 的恢复也不存在恢复部分文件的情况，因为 IOS 本身就是一个镜像文件。

1) 获取最新的 IOS 版本

新版本的 IOS 可以从供应商、思科网站及一些第三方工具等渠道获得。例如 IOSHunter, IOSHunter 是一款可以在网上自动查找对于路由器或交换机合适的 IOS Image 的工具, 操作方法非常简单, 图 6-5 为 IOSHunter 的操作界面。

在选择新的 IOS 软件时要考虑下面两个因素:

(1) 降低成本

现有网络设备中的 FLASH/DRAM 一旦不满足大尺寸 IOS 的要求, 不得不采购新的 FLASH/DRAM, 这会带来成本开销和一定的采购周期。

(2) 运行稳定

新的 IOS 如果刚刚问世不久, 也许会有新的安全漏洞和不稳定因素。对于企业生产网络来说, 稳定、连续运行才是我们追求的目标, 而不是功能齐全但暂时超出我们所需的软件, 更不必说这些太新的软件会带给生产网的潜在风险。所以, 最新的软件不一定稳定可靠, 我们需要的是被广泛使用了一段时间并且被证明能够稳定运行、消除了大量 BUG 的软件, 而且尽量选择与现有软件主版本号一致的软件。

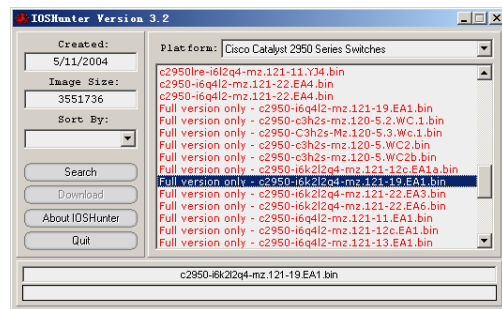


图 6-5 IOSHunter IOS 搜索工具

2) 确认升级范围与顺序

在此步骤中, 以 Cisco 的网络设备为例, 主要是要确认有安全漏洞的 IOS 软件版本和受影响的设备范围。首先从 Cisco 网站上查出有安全漏洞的 IOS 软件版本及替代版本。其次, 根据 IT 资产数据库, 确定受影响的硬件设备范围。

根据企业网络环境、数据流向及业务特点分析, 需要确定升级原则, 即首先升级次要节点中的次要设备, 再升级主要节点中的次要设备, 然后升级次要节点中的主要设备, 依此类推。

之所以先升级次要节点的次要设备, 是因为无法预测在实际升级后的生产网运行期间还会出现什么未知问题。而首先升级最次要的设备, 即使真的出现问题, 相对其他主要节点的影响而言, 它对用户业务的影响也会小些。换句话说, 次要节点可以作为整体升级的“试验田”, 一旦出现问题, 使我们有机会回退并降低风险和项目压力, 后续的升级也可以及时中止。

3) 评估 FLASH/DRAM 容量

对于新的替代 IOS 软件, 其文件尺寸往往大于旧的软件, 此时需要在升级前检查网络设备的 Flash/DRAM 的有效容量是否满足新 IOS 软件的运行要求。Flash/DRAM 的有效容量有以下两种情况:

(1) 容量大

当 Flash/DRAM 的有效容量可同时容纳两个 IOS 软件时, 可以在不删除旧 IOS 软件的情况下将新 IOS 软件上传到即将升级设备的 Flash 卡中, 这是最理想的情形。其好处是: 当升级失败时, 可以立即回退启用原来的 IOS 软件, 降低升级过程中的风险。

(2) 容量小

有效容量只能容纳一个 IOS 软件时, 上传新的 IOS 软件前需要删除旧的 IOS 软件, 然后重新启动网络设备, 这可能带来一定的风险, 一旦重启失败, 需要现场人工干预重新启用旧的 IOS 软件。

4) 物理准备

在升级操作过程中, 切记不可断电, 所以需要配置 UPS (不间断电源) 供电。另外, 使用的物理线路也需要提前测试, 保证其传输性能稳定。

5) 操作准备

绝大部分的升级工作都需要管理员直接接触到网络设备, 准备操作的平台 (台式机、笔记本均可), 用于对交换机进行配置操作及作为 TFTP 服务器存储 IOS 文件, 以及连接设备的直通线和 Console 线。

6.3.3 升级与恢复方案

如果是通过网络升级 IOS，运行 TFTP Server 主机连接交换机的接口没有限制，TFTP Server 的地址可以随意定义，但必须与网络设备定义的地址在同一网段上。连接至路由器时，必须使用路由器的第一个以太网口，即 Ethernet0（对 Cisco 2500 系列等）和 Ethernet0/0（对 Cisco 2600 系列等），其他系列略有差别，可根据使用手册进行确定。下面将详细介绍 IOS 文件修复的步骤。

1. 部署 TFTP

首先需要安装 TFTP Server 软件，这里使用 Cisco TFTP Server 的 TFTP 服务器软件，可以从 Cisco 网站下载。Cisco TFTP Server 的配置十分简单，几乎不用更改它的配置，如需要可以更改其根目录，在图 6-6 中的位置中选择。

将 IOS 文件放在 TFTP Server 所在目录的根目录下，如果 TFTP Server 软件在机器装的是 Cisco TFTP Server 目录，那么就把新的 IOS 文件放在 Cisco TFTP Server 目录下就可以了。也可以自行指定 IOS 文件的存放位置，

在 TFTP Server 软件界面上选择【View】→【Options】命令，在图 6-7 中“TFTP Server root”选项上选择“Browse”，将该目录指向 IOS 文件所在的目录，如 D:\cisco 或其他目录。

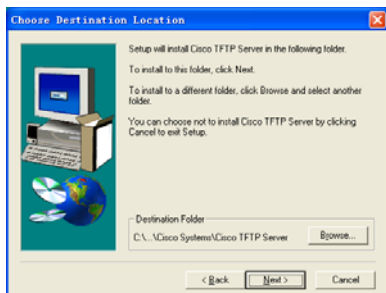


图 6-6 安装 TFTP 的位置

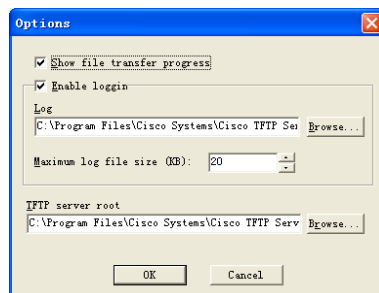


图 6-7 设置 TFTP 的根目录

2. 升级交换机 IOS

首先，用 Console 连接交换机的 Console 口与电脑的 COM1 口（或 USB 口，依据配置线不同而定，设置方法请查看第 5 章的相关内容），网线连接交换机 Fast Ethernet0/1 口与计算机的以太网口，打开 TFTP 服务器软件，并将其根目录设为 IOS 文件所在的目录。

为使交换机能与 TFTP 服务器相互通信，需要为交换机和 TFTP 服务器设置 IP 地址。

1) 设置 TFTP 服务器地址

首先需要将运行 TFTP 的计算机 IP 地址设为 192.168.0.1，如图 6-8 所示。

2) 设置交换机 IP 地址

使用 Windows 自带的超级终端软件，将交换机的地址设为与计算机的 IP 地址相同网段。三层交换机可以针对接口设置 IP，而二层交换机需要针对升级用 VLAN，设置 IP 地址。具体步骤如下。

第 1 步：进入全局配置模式

```
Switch#configure terminal
```

第 2 步：进入管理 VLAN 接口模式

```
Switch(config)# interface vlan 99
```

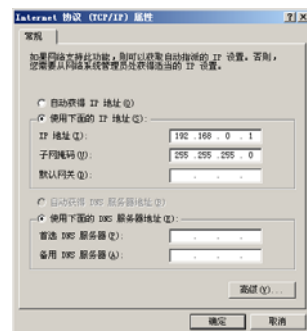


图 6-8 设置运行 TFTP 服务器的 IP 地址

第 3 步：配置 IP 地址

```
Switch(config-if)# ip address 192.168.0.2 255.255.255.0
```

第 4 步：将 Fasethernet 0/1 划分到 VLAN

```
Switch(config-if)# interface fasethernet 0/1
```

```
Switch(config-if)# witch access vlan 99
```

第 5 步：退回全局配置模式

```
Switch#exit
```

此时，如果能够在超级终端界面上 Ping 通 192.168.0.1，就表明交换机和 TFTP 服务器（电脑）连接与通信正常了。

3) 备份旧 IOS

在特权模式下输入 Show Flash 命令，查看当前交换机 Flash 内 IOS 的文件名：c2950-c3h2s-mz.120-5.3.WC.1.bin 及相关信息。在升级前，需要将这份 IOS 文件备份出来，以防在升级中出现意外无法恢复到初始状态。

```
Switch#copy flash tftp
Source filename []?c2950-c3h2s-mz.120-5.3.WC.1.bin //输入 IOS 文件名
Address or name of remote host []? 192.168.0.1 //输入 TFTP 地址
Destination filename [c2950-c3h2s-mz.120-5.3.WC.1.bin]?//可以更改名称或使用默认
```

4) 删除旧 IOS

复制的时间和 IOS 的大小有关，请耐心等待。备份完成后，就要将新的 IOS 文件复制到 flash 中。但通过 show flash 命令发现 Flash 中的剩余存储空间比要升级的 IOS 文件要少，为了使新的 IOS 文件能拷入交换机的 Flash 中，必须要先删除原 IOS 文件。

```
Switch#delete flash: c2950-c3h2s-mz.120-5.3.WC.1.bin //复制文件从 Flash 到 tftp
Delete filename [c2950-c3h2s-mz.120-5.3.WC.1.bin] //确认，回车
Delete flash:c2950-c3h2s-mz.120-5.3.WC.1.bin? [confirm] //确认，回车
```

5) 升级新 IOS

确认 Flash 中的 IOS 文件已经删除，在新的 IOS 文件被复制到交换机之前，一定要确保交换机不会重新启动，否则交换机就无法正常启动了。

```
Switch#copy tftp flash: //复制文件从 tftp 到 flash
Address or name of remote host []? 192.168.0.1 //输入 TFTP 地址
Source filename []? c2950-i6k2l2q4-mz.121-22.EA8a.bin //输入升级的新版 IOS 名称
Destination filename [c2950-i6k2l2q4-mz.121-22.EA8a.bin]? //确认，回车
```

新的 IOS 文件成功复制到 Flash 中之后，输入 reload 重启交换机。如果交换机能够正常的重启，查看 Flash 中的 IOS 文件已经变成 c2950-i6k2l2q4-mz.121-22.EA8a.bin。至此，IOS 的升级工作完成，最后可以删除临时性的 VLAN。

3. 使用 TFTP 修复路由器的 IOS

装有 TFTP Server 软件的 PC，在 PC 上启动 TFTP Server 软件，并把用控制线将调试机器与路由器连接起来。用 TFTP 修复 IOS 可以分为以下几个步骤。

第 1 步：设置路由器的 IP 地址，TFTP 软件所在的机器必须在同一网段内。

第 2 步：设置路由器的子网掩码。

第 3 步：设置默认网关地址（可忽略，或者指向 TFTP Server）。

第 4 步：设置 TFTP 服务器 IP 地址。

第 5 步：指定需要恢复的 IOS 名称。

第 6 步：确认执行恢复，执行 tftpdnld。

ROMMON 区分命令的大小写，请注意前面的几条命令必须使用大写，而最后的 tftpdnld 则要用小写。设置完后要用 sync 命令保存环境变量到 NVRAM。用 set 命令进行查看设置，具体恢复步骤如下：

```
rommon 2 > IP_ADDRESS=172.16.0.1
rommon 3 > IP_SUBNET_MASK=255.255.255.0
rommon 4 > DEFAULT_GATEWAY=172.16.0.2
rommon 5 > TFTP_SERVER=172.16.0.2
rommon 6> TFTP_FILE=c2600-is-mz.113-2.0.3.Q
rommon 7 > tftpdnld
IP_ADDRESS: 172.16.0.1
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 172.16.0.2
TFTP_SERVER: 172.16.0.2
TFTP_FILE: c2600-is-mz.113-2.0.3.Q
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n: [n]: y
Receiving c2600-is-mz.113-2.0.3.Q from 172.16.0.2 !!!!!!!
File reception completed.
Copying file c2600-is-mz.113-2.0.3.Q to flash.
Erasing flash at 0x607c0000
program flash location 0x60440000
rommon 8 >
```

4. 使用 XMODEM 修复 IOS

IOS 升级失败的原因有很多，比如升级过程中网线松动、用来升级的 IOS 文件和设备不匹配、突然停电等。遇到上述情况，设备将无法启动。除 TFTP 修复 IOS 之外，下面介绍 XMODEM 恢复（升级）IOS 的方法，只是比起前一种更加复杂，传输速度也比较慢，所以不太常用。

1) 修复交换机

将交换机连接以后，控制台会出现交换机 IOS 丢失的界面。此时需要重新启动交换机，重新为交换机加电，此时，请按住交换机面板左侧的 Mode 键，进入 MINI 模式。

在超级终端输入 flash_init 会出现大量提示，继续输入 load_helper，输入复制指令 copy XMODEM: c2950-i6k2l2q4-mz.121-22.EA8a.bin。出现 Begin the XMODEM or XMODEM-1K transfer now...提示，系统提示不断出现 C 这个字母就可以开始传输 IOS 文件了。

选择超级终端中【传送】→【发送文件】命令，在协议选项中选择 XMODEM 或者 XMODEM-1K 协议，如图 6-9 所示，然后选择 IOS 文件，开始传送。



因为此前没有改变控制台的传输速率，所以传送得很慢，一个普通的 Cisco IOS 文件大致需要 50 分钟左右，请耐心等待。在修复路由器 IOS 中将介绍改变传输速率的方法。

文件传送结束后，在提示符下输入：boot（启用新的 IOS 系统）。经过几十秒钟，交换机就进入正常的状态了，这时查看 Flash，里面应该有了新的 IOS 文件，至此 IOS 恢复工作完成。

2) 修复路由器

IOS 丢失以后，所有的设备都会启动最小启动模式。由于 Cisco 3640 版本路由器恢复没有提供 tftpdnld 命令，只提供了 XMODEM 命令，使用方法与 Cisco 2600 系列相同。为了加快修复的速度，需要配置路由器 Console 口和超级终端软件的传输速率。

```
rommon 2 > confreg
do you wish to change the configuration? y/n [n]: y
enable "diagnostic mode"? y/n [n]: n
enable "use net in IP bcast address"? y/n [n]: n
disable "load rom after netboot fails"? y/n [n]: n
enable "use all zero broadcast"? y/n [n]: n
enable "break/abort has effect"? y/n [n]: n
enable "ignore system config info"? y/n [n]: n
change console baud rate? y/n [n]: y
```

```
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400
4 = 19200, 5 = 38400, 6 = 57600, 7 = 115200 [7]: 7
change the boot characteristics? y/n [n]: y
enter to boot:
0 = ROM Monitor
1 = the boot helper image
2-15 = boot system
[0]: 0
Configuration Summary
enabled are:
load rom after netboot fails
console baud: 115200
boot: the ROM Monitor
do you wish to change the configuration? y/n [n]: n
You must reset or power cycle for new config to take effect
rommom 2 > reset
```

在 enter rate: 部分, 需要选择 7, 用最大的 115200 速率的 XMODEM 传输。在输入 reset 命令之前, 需要重新定义串口传输速度, 如图 6-10 所示, 将超级终端里设置速率为 115 200, 否则会出现乱码。



图 6-9 设置传输协议



图 6-10 设置最大传输速率

关闭这个超级终端, 重新建立一个超级终端连接 (115200 速率), 系统重新启动后会出现:

```
rommon 1>
rommon 1> XMODEM -r
Do not start the sending program yet...
Invoke this application only for disaster recovery.
Do you wish to continue? y/n [n]: y
Ready to receive file ...
```

此时, 选择超级终端中【传送】→【发送文件】命令, 在协议选项中选择 XMODEM 或者 XMODEM-1K 协议, 选择 IOS 文件, 开始传送。

当传输完毕后, 重新启动路由后开始使用被恢复的 IOS。此时, 需要再次启动路由器, 将传输速度恢复到默认状态, 即在 enter rate: 部分选择 0, 即 9 600 的传输速度。