

破解电信光猫华为HG8120C关闭路由功能方法（无需telnet）

📅 发表于 2015-01-24 | 🔄 更新于 2020-07-23



昨天电信的工作人员来安装了电信的光纤宽带，使用的是华为 HG8120C 这款光电转换器与路由器一体机，这导致下级路由无法直接使用 PPPOE 拨号连接到互联网，且无法使用端口映射来实现外网访问。而华为开放给用户的 useradmin 这个账号基本就是给你看着玩的，什么设置都改不了。必须获取到 telecomadmin 这个超级用户的密码，才能换路由为桥接。这款光猫在连接光纤后已经被电信远程关闭了 telnet，无法直接获取，但还算可以曲线救国。下面介绍方法。注意：若本文方法不适用，请参看 2018 新版文章：<http://hiram.wang/huawei-hg8120c-telecomadmin-2018/>

🔗 摆脱电信控制

当你连接上光纤后，你的光猫就会被电信远程控制，修改 telecomadmin 账号的默认密码，关闭 telnet，甚至还可以监控你所发送的数据包，所以我们首先必须摆脱电信的控制才能继续操作。



Hiram

Dream is Possible

文章 229 标签 234



☰ 目录 0

1. 摆脱电信控制
2. 启动 telnet
3. 获取超级用户密码

若你的光纤猫还没有连接过光纤，建议你事先进入 telecomadmin 账号关闭远程控制，默认密码应该是：nE7jA%5m

- 1、将你的电脑通过有线直接连接到光猫的 LAN1 口，保证稳定的连接
- 2、拔掉除了电脑连接线以外的所有线缆，包括光纤线，接下来重启光猫

启动 telnet

为了拿到这款华为工厂工具，我在淘宝网花了 30 元购买，这里免费共享

- 1、下载恢复工具：<https://089u.com/file/994552-83922910>
- 2、运行这个 exe 程序，选择“维修使能”，并选择连接到光猫的网卡，接着点启动即可



- 3、接下来下面的发送进度这个进度条会有进度，这时候观察你的光猫指示灯（注意：一直保持光纤断开状态，切记不要连接光纤！），刚开始光信号灯会是红灯闪烁，等到光信号灯不亮，LAN1、LAN2、网络 E/G 三个灯长亮，这时即可按下工具的停止按钮，关闭工具 4、重启光猫

4. 登录超级用户并关闭远程
5. 路由模式修改为桥接模式
6. 配置路由器与端口映射

最新文章

PHPFuck ([+.^]) 原理分析及 PHP 5 支...
2021-02-05

PHP WebShell 静态免杀技术研究
2021-02-03

使用 SetToolKit 一键生成钓鱼网站
2021-02-03

内网渗透中 Responder 工具的应用
2021-02-03

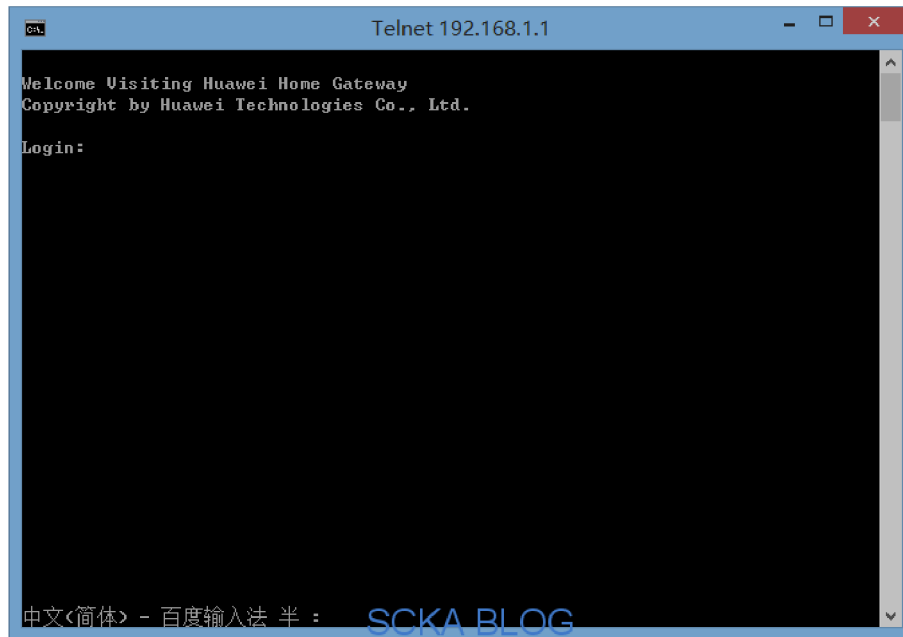
使用 Powersploit 实现 PowerShell 无...
2021-02-03

🔗 获取超级用户密码

重启完成重新连接到光猫，telnet 应该就被打开了 1、在 cmd 中输入下面的命令：

```
telnet 192.168.1.1
```

若提示 telnet 命令不存在，建议下载 putty，使用 telnet 模式连接 2、接下来会进入光猫 telnet 界面



3、输入下面的信息：

用户名：root 密码：admin

4、通过授权验证，接下来会进入控制界面



5、依次执行下面的命令

```
shell
```

```
cd /mnt/jffs2
```

```
ls
```

若看到下面的界面即为正常：

```

Telnet 192.168.1.1
MAP>shell
BusyBox v1.18.4 (2014-01-13 16:55:12 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

profile close core dump, flag=
MAP(Dopra Linux) # cd /mnt/jffs2
MAP(Dopra Linux) #
MAP(Dopra Linux) # ls
1.xml                  custunpara.txt          hwontdebuglogdata.bin
2.xml                  cwmpr_rebootsave        hwontlog.bin
DHCPPlasterwan1       dhcpd                   main_version
DHCPPlasterwan2       emergencystatus         mount_ok
DHCPOutputwan1        eponroquestatus        oldcrc
DHCPOutputwan2        fsok                    ontstatusfile
DHCPStatewan1         ftvoipcfgstate          optic_init_par.bin
DHCPStatewan2         hard_version            optic_par_debug
FTCRC                 hw_boardinfo            ppplaster260
InformFlag            hw_boardinfo.bak        reboot_info
board_type            hw_bootcfg.xml          recovername
ceaseadv.conf         hw_ctree.xml            roquestatus
cu_cfg_counter        hw_ctree_bak.xml        xmclfgerrorcode
customize.txt          hw_default_ctree.xml
customizepara.txt      hwontdebuglogctrl.bin
MAP(Dopra Linux) #
MAP(Dopra Linux) #
中文(简体) - 百度输入法 半 : SCKA BLOG
  
```

6、继续执行下面的命令获取密码：

```

cp hw_ctree.xml myconf.xml.gz
aescript2 1 myconf.xml.gz tmp
gzip -d myconf.xml.gz
  
```

正常反馈如下：

```

MAP(Dopra Linux) # cp hw_ctree.xml myconf.xml.gz
MAP(Dopra Linux) #
MAP(Dopra Linux) # aescript2 1 myconf.xml.gz tmp
MAP(Dopra Linux) #
MAP(Dopra Linux) # gzip -d myconf.xml.gz
MAP(Dopra Linux) #
MAP(Dopra Linux) #
SCKA BLOG
  
```

7、经过复制、解密、解压，现在密码就已经被破译出来了，保存在 myconf.xml 中，需要查看的话运行下面的命令：

```
grep telecomadmin myconf.xml
```

会出来下面的一串字符：

```

MAP(Dopra Linux) # grep telecomadmin myconf.xml
<X_HW_WebUserInfoInstance InstanceID="2" UserName="telecomadmin" Password="
a" UserLevel="0" Enable="1" PasswordFlag="1"/>
SCKA BLOG
  
```

其中 Password = 后面就是我们寻觅已久的超级用户密码，将它复制出来保存好，若你会 vi 命令，理论上也可以改密码，详见：

<http://www.xcar.com.cn/bbs/viewthread.php?tid=19728461>

- 1、现在断开 telnet，直接进入后台管理界面，输入刚刚的用户名和密码（不要连接光纤）



- 2、你会发现设置项目变得专业和强大了不少，进入网络 - 远程管理，取消“使能周期通知”复选框，点击“应用”，彻底切断电信的远程控制



ACS参数设置

如果TR069的自动连接功能是使能的，您可以设置终端的ACS变量参数。

使能周期通知:	<input type="checkbox"/>
周期通知时间间隔:	43200 * [1 - 2147483647](s)
周期通知时间:	yyyy-mm-ddThh:mm:ss(例如:2009-12-20T12:23:34)
ACS URL:	http://devacs.edatahom *
ACS用户名:	hgw *
ACS密码: * (密码的长度必须在1~256位字符之间)
请求连接的用户名:	itms *
请求连接的密码: * (密码的长度必须在1~256位字符之间)

应用 取消

- 3、连接上光纤以及一切你要连接的线，测试网络 / IPTV / 语音是否正常，理论上不会有任何影响

🔗 路由模式修改为桥接模式

这设置再强大终究还是不如我们的路由器可靠，我们需要关掉光猫的路由功能，才能实现完全的自由 1、进入后台 - 网络 - 宽带设置，选择“4_INTERNET_B_VID_1117”



2、将连接类型由“路由 WAN” 改为“桥接 WAN”



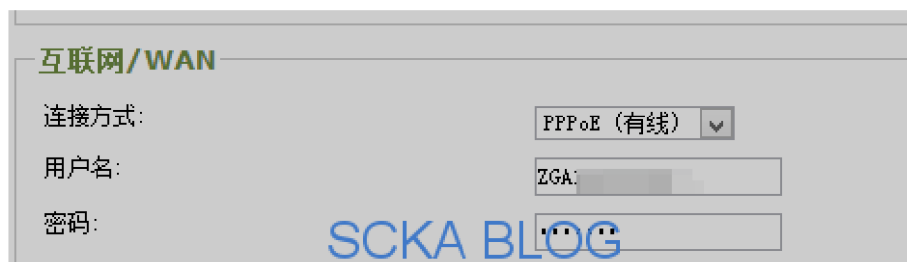
特别注意：在修改为路由器拨号后，我们必须知道自己宽带的账号密码才行，账号在光猫中能看到，而密码很多都是加密存储，无法获取，若你不知道密码，可以打 10000 询问，或者在这个网址进行密码重置：

http://sc.189.cn/service/pwdReset/pwdReset_KD.jsp（四川地区，其他地区自行查找）

3、点击“应用”按钮，稍等一会，网络便会断开

配置路由器与端口映射

1、接下来断开电脑，在光猫下连接好路由器 2、进入路由器的 PPPOE 设置界面（注意路由器网关不能设置为 192.168.1.1，否则会与光猫冲突），输入你的宽带账号密码，确认拨号即可上网！



广域网IP地址:

125.66.169.219

广域网子网掩码:

255.255.255.255

广域网MAC地址:

40:16:9F:BA:00:19

广域网网关IP:

125.66.168.1

广域网DNS服务器:

8.8.4.4

8.8.8.8

广域网（PPPOE）连接时间:

0天 1小时, 24 分钟

SCKA BLOG

至此，我们已经完全摆脱电信的控制，获得了最高控制权，获得了完全的自由！ 3、对应的，端口映射和动态域名之类的全都可以用了，看起来电信并没有封锁 80 端口

我的IP

网页 新闻 贴吧 知道 音乐 图片 视频 地图 文库 更多»

百度为您找到相关结果约100,000,000个

IP地址查询

iP

本机IP: 125.66.169.219 四川省自贡市 电信

请输入ip地址

查询

本机IP查看方法

IP地址设置方法

SCKA BLOG

125.66.169.219/login.sh

Gargoyle

状态
连接
防火墙
系统
注销

登录

输入管理员密码:

登录

当前日期和时间

01/24/15 下午 12:24 UTC+8

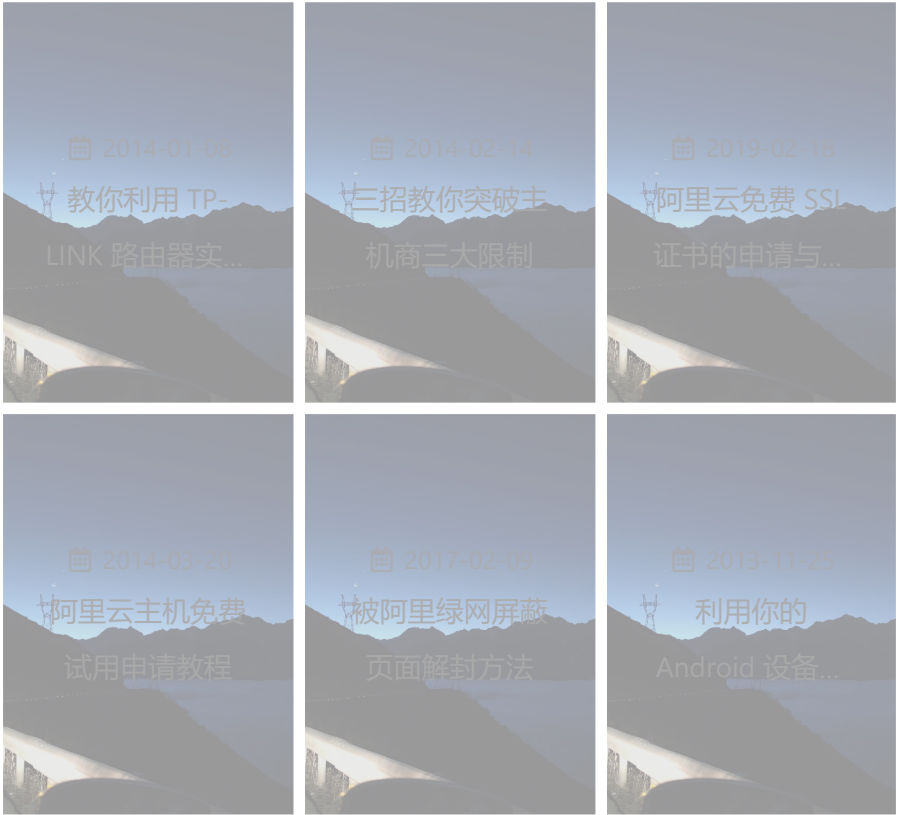
SCKA BLOG

4、大获全胜！

- 技术经验
- 网站建设
- 路由器
- 电信光猫



👍 相关推荐



💬 评论

昵称

邮箱

欢迎留下你的见解

表情 | 预览

回复

快来做第一个评论的人吧~

Valine XSS Fixed By [Hiram](#)

©2013 - 2021 By Hiram

Powered by Hexo | Theme Butterfly

本站所有头图版权均归博主所有，未经许可，禁止使用

蜀ICP备15021023号-3 本站由阿里云提供全站加速和对象存储服务