烽火通信科技股份有限公司
FIBERHOME TELECOMMUNICATION TECHNOLOGIES CO.,LTD.

BCM6848 家庭网关使用及调测说明

版本：A
代号：
日期：2015-09

烽火通信科技股份有限公司

FIBERHOME TELECOMMUNICATION TECHNOLOGIES CO. LTD

目　　录

0　版本记录 3
1　目的 3
2　适用范围 3
3　WEB 页面 3
3.1　管理员 WEB 页面 3
3.2　出厂设置隐藏 WEB 页面 3
3.3　LOGOFFACCOUNT 页面 8
4　串口和 TELNET 9
4.1　串口相关命令 9
4.2　TELNET 10
5　通用调试方法 10
5.1　通过串口或 TELNET 获取调试打印信息 10
5.2　端口镜像抓取相关报文 12
5.3　配置文件 12
6　故障排查 13
6.1　TR069 13
6.2　WEB 13
6.3　语音 14
6.4　QOS 14
6.5　NTP 15
6.6　OAM 16
6.7　CFE 17
6.8　性能 17
6.9　IPv6 18
6.10　内核 19
6.11　组播 19
6.12　数据接口 19
7　Q&A 24

0 版本记录

序号	版本号	生成时间	主 要 修 改 记 录	作者	备注
1	RA	2015-09-12	初稿	侯彦超	
2					
3					

1 目的

博通 6848 方案是基于博通的 6848 芯片设计开发，主要有 EPON 和 GPON 两种上行方式。该方案是在我司博通 6838 方案的基础上开发新的网关产品形态，最终实现新老网关更替。本文档主要介绍博通 6848 方案下 HG2XXGU 系列家庭网关的使用及调试方法，以及常见故障的排查方法。

2 适用范围

本手册适用的人员为：中试人员、工程人员。

本手册适用的范围为：BCM6848 方案自研设备，其中包括 HG220GS-U、HG260GS-U，HG22XGU,HG26XGU 系列。

本文以联通定制版本为基础进行介绍，使用博通 6848 方案的其他运营商版本相关调测说明雷同，本文不再进行赘述。

3 WEB 页面

3.1 管理员 WEB 页面

在浏览器地址栏输入 http://192.168.1.1/cu.html

联通维护账号：CUAdmin

联通维护账号密码：CUAdmin

以上信息全国各省份不统一，还需以具体省份要求为准。

3.2 出厂设置隐藏 WEB 页面

在浏览器地址栏输入 http://192.168.1.1

账号：fiberhomehg2x0

密码：hg2x0

3.3 MAC 及序列号

进入“出厂设置—基本设置”界面（图 3-1）：

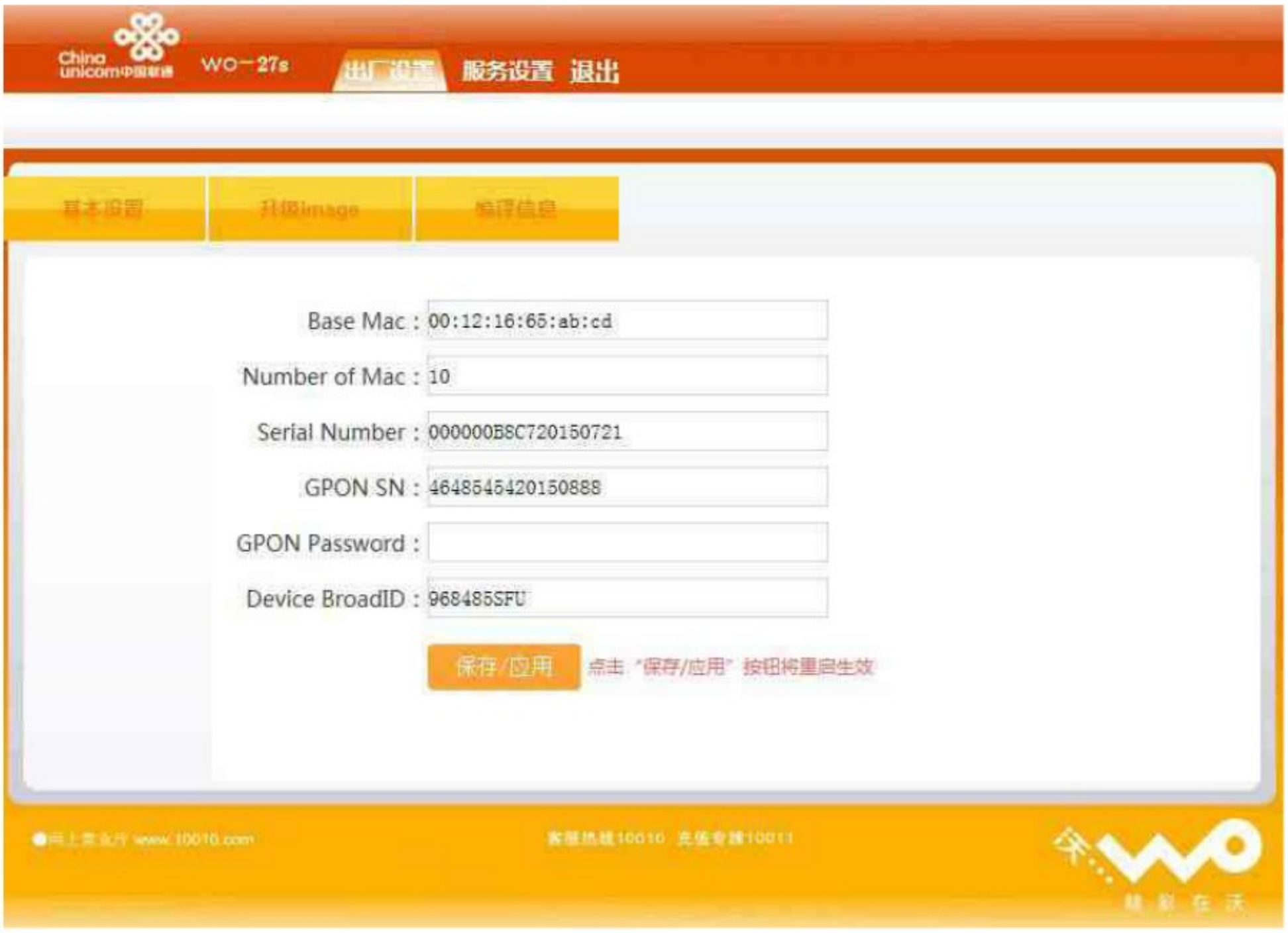

图 3-1

每台 HG2XXG 网关占用 10 个 MAC 地址，此处显示的是设备的 Base Mac，ONU MAC 为 Base Mac+9，MAC 地址的前 6 位（例如 b8:c7:16）的大写（B8:C7:16）作为设备的厂家 OUI 信息，在向平台进行注册前，请与平台方确认需将 ONI 信息在平台上增加才能注册成功。Serial Number 为设备序列号后缀。

GPON SN 和 GPON Password 是在设备出厂时就配置好的（只有 GPON 上行的网关有），在 OLT 注册后显示为物理地址用的，它的命名规则为 46485454+basemac 后 8 位(大写)，其中 46485454 为字符串 FTTH 的 ascii 码；

Device BroadID 为设备的 broadid，GPON 的设备可以通过在隐藏页面里面修改 boardid 切换成 EPON，但是切换后，需要在串口下执行 restoredefault 命令清空配置。但是 EPON 设备不能切换成 GPON（EPON 光模块不支持），同时不同形态的设备不能切换，如 4+2 的设备切换成 2+1 等

型号	类型	端口数量	BoardIdNo	BoardId
HG260GS	GPON	4	0	968380FHGU
HG261GS	GPON	2	14	968385SFU
HG220GS	EPON	4	11	968380FEHG
HG221GS	EPON	2	15	968385ESFU

3.4 软件升级

进入“出厂设置—升级 image”界面（图 3-2）：

图 3-2

请确保升级程序的时候，一定要依次执行下面三个操作步骤：

1、系统镜像文件升级；

2、通用预配置导入；

3、预配置生成。

以上三个步骤必须按照顺序连贯操作（中间不能再修改 wan 连接、语音配置等），特别是第三步，否则后面”恢复预配置”会达不到预期的效果（恢复为设备之前生成过的其他省市预配置）。

另外以上 2、3 步骤也可通过在 telnet 中输入预配置导入命令来代替，以达到更新预配置的效果。

3.5 软件版本查询

进入“出厂设置—编译信息”界面（图 3-3）：

图 3-3

此页面主要提供软件编译日期、SVN 版本号等软件版本相关信息。

3.6 应用服务

进入“服务设置—应用服务”界面（图 3-4）：

图 3-4

此页面主要提供 FTP、TELNET 服务开启和关闭功能，开启后默认的用户名和密码均为 admin。

3.7 日志下载

进入“服务设置—日志下载”界面（图 3-5）：

图 3-5

此页面提供语音及 OMCI、OAM 等日志的下载提取功能（操作与博通 6838 方案类似）。

3.8 logoffaccount 页面

在浏览器地址栏输入 http://192.168.1.1/logoffaccount.html（实际地址以具体分省为准）进入如下界面（图 3-6）：

图 3-6

账号登陆状态管理：

此页面提供 CUAdmin 和 useradmin 账号登录状态的注销功能。

Httpd 配置：

此页面提供 TR069 相关参数修改权限以及控制隐藏用户 fiberhomehg2x0 是否启用的功能。

注册过程修改：

此页面提供终止正在向 ITMS 发起的注册，允许重新进行注册的功能（部分省份有此需求）。

4 串口和 TELNET

4.1 串口相关命令

设备接上串口后，如图 4-1 设置串口波特率等参数：

图 4-1

串口登陆后，默认进入 CLI 命令行 “>”模式。

输入 sh 命令，可以进入 SHELL 命令行“#”模式，exit 退出 SHELL 命令行模式，回到 CLI 命令行模式。两种模式下输入不同的命令行可以实现不同的功能。（图 4-2）

```
 > sh


BusyBox v1.17.2 (2013-12-10 16:49:12 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

#
#
# exit
 > help
?
help
logout
exit
quit
reboot
brctl
cat
virtualserver
ddns
df
loglevel
logdest
dumpcfg
dumpmdm
dumpeid
mdm
meminfo
psp
kill
dumpsysinfo
dnsproxy
syslog
echo
ifconfig
ping
ps
```

图 4-2

CLI 命令行主要用于设置模块调试信息打印级别和获取 dump 配置，SHELL 命令行作用与 HG22X 设备类似，主要用于查看日志文件及配置文件、开启端口镜像命令等。

4.2 TELNET

TELNET 用户名和密码均为 admin，与串口功能基本类似。但默认状态下 TELNET 输出的相关调试打印信息比串口少很多，条件允许时建议尽量使用串口进行调试。

5 通用调试方法

HG2xxGS 系列产品通用调试方法和调试信息收集主要有 3 种：调试打印、配置文件、端口镜像抓包。

5.1 通过串口或 TELNET 获取调试打印信息

（1）串口日志调试级别设置

在 CLI 命令行输入 loglevel help 命令，查询相关命令格式。（图 5-1）

```
>loglevel help
usage: loglevel get appname
       loglevel set appname loglevel
where appname is one of: httpd, tr69c, smd, ssk, telnetd, sshd, consoled, upnp, dnsproxy, osgid,
vodsl, fhvoice, cpmngr, apimngr
loglevel is one of "Alert","Error", "Notice", or "Debug" (use these exact strings).
```

图 5-1

以设置 httpd 日志级别为 Debug 为例（图 5-2）：

1、 loglevel get httpd 对当前 httpd 日志级别进行查询（默认为 Error 级别）；

2、 loglevel set httpd Debug 设置 httpd 日志级别为 Debug（常用调试级别）；

3、 调试完毕后，loglevel set httpd Error 将日志级别改回 Error,以免影响设备性能；

4、 对日志级别设置完成后，输入 save 命令可使设置的调试级别一直生效，如果不保存，重启后日志级别会恢复为 Error 级别。

```
 > loglevel get httpd
current log level is Error
 > loglevel set httpd Debug
new log level set.
 > loglevel get httpd
current log level is Debug
 > loglevel set httpd Error
new log level set.
 >
```

图 5-2

（2）TELNET 调试日志级别设置

在不具备串口接入条件的情况下，可以采用将串口日志从 TELNET 输出的方式，但仍有少量信息 TELNET 无法输出。

登陆 TELNET，在 CLI 命令行输入 logdest help 命令，查询相关命令格式。（图 5-3）

```
>logdest help
usage: logdest get appname
       logdest set appname logdest
where appname is one of: httpd, tr69c, smd, ssk, telnetd, sshd, consoled, upnp, dnsproxy ,fhvoice,
cpmngr, apimngr
loglevel is "Standard Error", "Syslog" or "Telnet".
```

图 5-3

以设置 httpd 日志级别为 Debug,并将相关日志在 TELNET 输出为例（图 5-4）：

1、 loglevel set httpd Debug 设置 httpd 日志级别为 Debug（常用调试级别）；

2、 logdest set httpd TELNET 设置 httpd 相关日志在 TELNET 输出；

3、 调试完毕后，loglevel set httpd Error 将日志级别改回 Error,以免影响设备性能；

4、 对日志级别设置完成后，输入 save 命令可使设置的调试级别一直生效，如果不保存，重启后日志级别会恢复为 Error 级别。

```
> loglevel get httpd
current log level is Error
 > loglevel set httpd Debug
new log level set.
 > logdest set httpd Telnet
new log dest set.
 > httpd:617.762:web_main:2129:url_address=::ffff:192.168.1.1
httpd:617.763:web_main:2135:client ip=::ffff:192.168.1.3
httpd:617.763:cmsLck_acquireLockWithTimeoutTraced:94:acquired l
httpd:617.764:cmsDal_getNetworkAccessMode6:134:returning access
httpd:617.764:cmsLck_releaseLockTraced:139:lock hold time=0ms,
```

图 5-4

5.2 端口镜像抓取相关报文

在操作设备的同时，使用 Wireshark 抓取相应模块所要求的报文。

目前芯片只能支持 WAN 侧到 LAN 侧的端口镜像，不支持 LAN 到 LAN 的端口镜像。

进入 SHELL 命令行模式，在串口依次输入以下端口镜像命令：

bs /b/con port/index=wan0 mirror_cfg={rx_dst_port={port/index=lan3},tx_dst_port={port/index=lan3}}

（将 PON 口镜像到设备 LAN1 口）

lan3 对应设备 LAN1 口，(LAN2-4 口分别对应 lan2、lan1、lan0)。

设备重启后端口镜像自动关闭。也可以使用如下命令手动关闭关口镜像命令：

bs /b/con port/index=wan0 mirror_cfg={rx_dst_port=null,tx_dst_port=null}

5.3 配置文件

使用 dumpmdm/dumpcfg 导出当前 MDM/PSI 中的配置信息。

通过命令行方式，开启 SecureCRT/ Tera Term 的日志记录功能，如果具有时间戳也一并开启，在 CLI 模式>后执行：

```
>dumpcfg                    #导出当前 PSI（即 Flash 配置）
>dumpmdm                    #导出当前 MDM（即共享内存配置）
```

也可通过页面方式，登陆 WEB 页面后，在地址栏输入：

http://192.168.1.1/dumpcfg.cmd

http://192.168.1.1/dumpmdm.cmd

6 故障排查

6.1 TR069

通过 loglevel set tr69c Debug 打开 tr069 模块的日志，若需要重启后也生效，输入 save 命令即可。如果要关闭 tr069 模块的日志，通过 loglevel set tr69c Error，同时回车后还需输入 save 命令。

可以通过串口设置网关参数节点的值，格式如下

itms set “网关参数全路径名” “设置值的类型” “设置的值”

例如

itms set InternetGatewayDevice.Services.VoiceService.1.LoggingLevel s Debug

通过串口获取网关参数节点的值如下

Itms get “网关参数全路径名”

itms get InternetGatewayDevice.Services.VoiceService.1.LoggingLevel

6.2 WEB

1、 查看页面源代码：IE：鼠标右键点击“查看源文件”（图 6-1），html 代码将以默认编辑器打开。Firefox：通过插件 firebug 或者地址栏输入 view-source:[host-ip]/[file-name]（例如 view-source:http://192.168.1.1/ctwanconfig.html）。

图 6-1

2、打开 httpd 日志：CLI 命令行输入 loglevel set　httpd Debug

logdest set httpd [log_dest] 说明：默认为 Standard Error,即串口，如果多个程序的日志，避免干扰，也可输出到 Telnet,如果 Telnet 未开启，使用 fiberhomehg2x0/hg2x0 帐号下的“服务设置->应用程序”页面开启 Telnet 应用。

3、查看 mdm 中信息：CLI 命令行：dumpmdm; 页面查看:[host-ip]/dumpmdm.cmd

4、注销帐号和 Tr069 禁用修改：[host ip]/logoffaccount.html

5、抓取 http 包：打开 PC 上的 wireshark, 选择合适的网卡，抓包，Filter 输入 http 作为过滤。

6、在联通维护账户 CUAdmin 下的 DHCP 页面修改配置后会注销当前所有帐号的登录信息，所以需要重新登录。在联通维护账户 CUAdmin 和普通用户账户 useradmin 修改用户 useradmin 的账户信息后，会注销 useradmin 的登录信息。

如果在页面上做其它操作（非用户注销操作），出现“用户已注销，请重新登录”之类的提示用户需要重新登录的信息，一般都是先前的操作执行中出现了某些问题。如果此问题能重现，则抓取 httpd 日志和 mdm 记录，便于分析。

7、无法打开 web 页面时，首先确保 PC 和设备之间的通信是否 OK，地址栏的输入是否正确，再去串口或 telnet 查看 ps 结果中是否有 httpd 进程的记录，如果没有，一般是 ssk 出现问题。重启设备如果现象依旧，则另作别论。

6.3 语音

SIP 模块及语音驱动调试方法：

1、开启端口镜像，抓包

2、设置调试级别为 Debug,获取日志/var/SipAppLog.txt、/var/SipLog.txt 和/var/AudioDrive.txt

3、获取串口输出信息。

4、在 CLI 接口中输入启动和停止 pcm 录制命令：

recordpcmstart——启动 pcm 录制。挂机后获取 /var/egCap0.raw /var/ingCap0.raw /var/egCap1.raw /var/ingCap1.raw

recordpcmend——停止 pcm 录制。

5、通过 WEB 获取 MDM 信息：http:ip/dumpmdm.cmd

H.248 调试方法：

1、开启端口镜像抓包，看流程是否正确。

2、设置调试级别为 Debug，获取日志 /var/MegacoAppLog.txt 和 /var/MegacoLog.txt 、/var/AudioDrive.txt。

3、通过 WEB 查看 H.248 相关的 MDM 信息是否配置正确。

6.4 QOS

1、观察 mdm 里相应的 class、app 模板类型等与设置是否一致。

2、用 ebtables -t broute -L 、ebtables -t nat -L 及 iptables -t mangle -L –n（图 6-3）观察后台命令是否正确。

```
# ebtables -t broute -L
Bridge table: broute

Bridge chain: BROUTING, entries: 1, policy: ACCEPT
-p IPv4 --ip-proto 6 --ip-dport 200 -j mark --mark-or 0x800 --mark-target ACCEPT
# ebtables -t nat -L
Bridge table: nat

Bridge chain: PREROUTING, entries: 0, policy: ACCEPT

Bridge chain: OUTPUT, entries: 0, policy: ACCEPT

Bridge chain: POSTROUTING, entries: 1, policy: ACCEPT
--mark 0x800/0x7f800 -j rule1

Bridge chain: rule1, entries: 5, policy: ACCEPT
-o eth0.0 -j RETURN
-o eth1.0 -j RETURN
-o eth2.0 -j RETURN
-o eth3.0 -j RETURN
-j mark --mark-or 0x803 --mark-target CONTINUE
# iptables -t mangle -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MARK       all  --  anywhere             anywhere            mark match 0x800/0x7f800 MARK or 0x803
#
```

图 6-3

3、最直观的方法是抓包，看抓到的包是否按预想被打上各种标记。

6.5 NTP

1、打开 loglevel set httpd Debug（串口下有效）

2、页面配置校时后，串口或 telnet 进网关，date 命令查看网关时间是否正确（图 6-4）；

```
#
# date
Thu Sep 27 11:28:06 UTC 2012
#
```

图 6-4

3、步骤 2 后，如果发现时间不正确，通过如下命令（图 6-5）经打印查看 ntp 同步时间是否可以成功：

如果 ntp 绑定了 internet wan 链接： ntpdate -d ntpserver

如果 ntp 绑定了 tr069wan 链接： ntpdate -d -9 ntpserver

如果 ntp 绑定了 voip wan 链接： ntpdate -d -8 ntpserver

```
# ntpdate -d ntpserver
 1 Jan 00:09:18 ntpdate[3230]: ntpdate 4.2.4p5@1.1541 Fri Aug 17 07:04:26 UTC 2012 (1)
Looking for host ntpserver and service ntp
Error : Name or service not known
 1 Jan 00:09:18 ntpdate[3230]: can't find host ntpserver

 1 Jan 00:09:18 ntpdate[3230]: no servers can be used, exiting
# 
```

图 6-5

注意：通过以上三个命令因为使用的-d(DEBUG)方式，如果时间同步成功，date 命令查看网关系统时间是不会被修改的，这三个命令只是可以通过打印看网关的 ntp 是否可以连接上 ntp server 进行时间同步。

如果使用如下三个不带 debug 命令，则可以通过打印大体观察到网关的 ntp 是否可以连接上 ntp server 进行同时间步，如果同步成功，则 date 查看网关的系统时间会被修改，但与实际时间会相差 8 个小时（8 个时区）。

如果 ntp 绑定了 internet wan 链接： ntpdate ntpserver

如果 ntp 绑定了 tr069wan 链接： ntpdate -9 ntpserver

如果 ntp 绑定了 voip wan 链接： ntpdate -8 ntpserver

6.6 OAM

三种方式获取 OAM 日志：

一：telnet 方式

将/tmp/eponapp.log_***取出 (*** 为随机数字)

二、网页方式

登陆隐藏页面， 服务设置->日志下载，下载 OAM 日志(下载的是/tmp/eponapp.log_***文件）

三、串口方式

（下面的步骤为重新复现后，搜集完整的串口日志）

1、断纤，设备重启

2、设备起来后，输入命令

>loglevel set eponapp Debug

>sh

#eponctl debug 1 2 1

4、在shell下 tail -f /tmp/eponapp.log***

5、最后插纤

6.7 OMCI

telnet 到设备，在交互模式下，输入 gponctl getState，查看输出的 operational state 是否为 O5。登陆隐藏页面， 在服务设置->日志下载栏目下，点击 bcm_omci.log 下载。下载日志分析。

6.8 CFE

1、若怀疑设备文件系统错误或 NVRAM 损坏，在 cfe 提示符下输入:dumpnvram 即可；

2、判断设备无线是否校准过：请核实/fhconf/wlan/bcm43217_map.bin 是否存在，存在表明该设备无线模块出厂已校准；

6.9 性能

1、开启关闭加速及查看相关信息(fap 和 flowcash)，默认加速开启

关闭加速： fc disable

打开加速： fc enable

查看加速状态： fc status

加速开启状态：

```
# fc status
        Flow Timer Interval<0xc04c7a0c> = 10000 millisecs
        Pkt-HW Activate Deferral<0xc04c7b74> : 1
        Pkt-HW Idle Deactivate<0xc04c7b78> = 1
        MCast Learning IPv4<Enabled> IPv6<Enabled>
        IPv6 Learning <Enabled>
        IP-Flow Learning Enabled : Max<16384>, Active<2>, Cummulative [ 470 - 468 ]
#
```

加速关闭状态：

```
Broadcom Packet Flow Cache learning via BLOG disabled.
# fc status
        Flow Timer Interval<0xc04c7a0c> = 10000 millisecs
        Pkt-HW Activate Deferral<0xc04c7b74> : 1
        Pkt-HW Idle Deactivate<0xc04c7b78> = 1
        MCast Learning IPv4<Enabled> IPv6<Enabled>
        IPv6 Learning <Enabled>
        IP-Flow Learning Disabled : Max<16384>, Active<9>, Cummulative [ 489 - 480 ]
#
```

3、清空加速表项

fc flush

一般关闭加速后需要清空加速表项，否则经过加速的数据流将继续通过硬件转发。

4、修改加速老化时间

fc config --timer 100000

加速老化时间单位是 ms，以上命令表示修改老化时间为 100 秒。一般默认的老化时间是 10 秒，通过 fc status 可以查看加速表项的老化时间（Flow Timer Interval 字段）。

5、查看加速表项

bs /b/e ip_class flow

```
# bs /b/e ip_class flow
Object: ip_class. Object type: ip_class. Owned by: system
==========================================
        flow[421] : [key=[src_ip=192.168.1.23,dst_ip=157.56.106.184,prot=17,src_port=62667,dst_port=3544,dir=us],result=[qos_meth
od=flow,action=forward,trap_reason=no_trap,dscp_value=0,nat_port=62667,nat_ip=10.96.20.29,dslite_src=::,dslite_dst=::,policer=null,p
ort=wan0,queue_id=0,wan_flow=5,ovid_offset=offset_12,opbit_action=dscp_copy,ipbit_action=dscp_copy,l2_offset=-4,l2_head_size=18,l2_n
um_tags=0,action_vec=ttl+nat,l2_header=00005e000166b8c7162121258100002a0800[15]]]
        flow[422] : [key=[src_ip=157.56.106.184,dst_ip=10.96.20.29,prot=17,src_port=3544,dst_port=62667,dir=ds],result=[qos_metho
d=flow,action=forward,trap_reason=no_trap,dscp_value=0,nat_port=62667,nat_ip=192.168.1.23,dslite_src=::,dslite_dst=::,policer=null,p
ort=lan0,queue_id=0,wan_flow=0,ovid_offset=offset_12,opbit_action=dscp_copy,ipbit_action=dscp_copy,l2_offset=4,l2_head_size=14,l2_nu
m_tags=0,action_vec=ttl+nat,l2_header=f0def17f7738b8c71621[3]0800[19]]]
MON: success
# 
```

以上图片显示网关当前有两条数据流经过硬件加速，key 标识了数据流的特征，分别由源 ip、目的 ip、协议、源端口号、目的端口号以及数据流的方向组成。图片中显示经过硬件加速的两条数据流特征如下：

src_ip=192.168.1.23,dst_ip=157.56.106.184,prot=17,src_port=62667,dst_port=3544,dir=us

src_ip=157.56.106.184,dst_ip=10.96.20.29,prot=17,src_port=3544,dst_port=62667,dir=ds

6、查看加速报文统计

bs /b/e port/index=wan0 stat

```
# bs /b/e port/index=wan0 stat
Object: port/index=wan0. Object type: port. Owned by: gpon
==========================================
                stat : [rx_valid_pkt=677,rx_crc_error_pkt=0,rx_discard_1=18,rx_discard_2=0,bbh_drop_1=0,bbh_drop_2=0,bbh_drop_3=0,rx
_discard_max_length=0,rx_discard_min_length=0,tx_valid_pkt=0,tx_discard=0,discard_pkt=0]
MON: success
# 
```

以上命令查看的是经过硬件加速转的 PON 口的报文统计，通过该命令可以看到网关是否有丢包。上行方向检查 tx_discard 是否有报文统计，下行方向检查 rx_discard_1 和 rx_discard_2 是否有报文统计。

注意：该命令每读一次则将上一次的统计清除，不会累加统计。

7、性能测试中的注意事项

1) 关闭 OLT ARP 代理使能

2) 关闭 OLT PON 口和上联口报文抑制，特别是单向性能测试时一定要关闭报文抑制，否则因为 OLT MAC 地址老化导致报文被抑制，影响测试结果。

3) 性能测试结果异常，比如 256 字节的性能比 512 好，在排除环境异常的情况下，很可能是在测试 512 字节时网关加速表项老化，报文经过 CPU 转发导致丢包，解决办法是重测时先打流让网关学习到加速表项，再开始测试。

4) 确保 OLT 上网关的带宽为最大值（1Gbps）

5) 一般 OLT 下挂的网关过多会影响被测网关的性能，测试时需保证测试环境干净，不受干扰，比如 OLT 仅下挂被测设备，上联口仅连接测试仪表

6) 多业务性能测试时需要关闭用户数限制

6.10 IPv6

1、打开日志： 设置 smd、ssk 日志等级为 Debug。

2、 抓包：ipv6 所有报文可用 ipv6 过滤：

测试 dhcp 可以用 dhcpv6 || icmpv6 过滤；

测试 pppoe ipv6 单栈或者双栈时可以用 icmpv6||ppp||pppoed||dhcpv6 过滤；

3、ipv6 相关的串口命令：

查看 ARP 表：ip -6 neigh

查看路由：route -A inet6 或者 ip -6 route；

查看地址：ifconfig

6.11 内核

串口通过 echo 8 > /proc/sys/kernel/printk 命令打开内核调试信息。默认内核打印级别为 8，只有当选择的级别大于下表（图 6-7）级别时，才会输出相应级别的内核打印信息。

```
#define KERN_EMERG "<0>" /* system is unusable */
#define KERN_ALERT "<1>" /* action must be taken immediately */
#define KERN_CRIT "<2>" /* critical conditions */
#define KERN_ERR "<3>" /* error conditions */
#define KERN_WARNING "<4>" /* warning conditions */
#define KERN_NOTICE "<5>" /* normal but significant condition */
#define KERN_INFO "<6>" /* informational */
#define KERN_DEBUG "<7>" /* debug-level messages */
```

图 6-7

6.12 组播

如果组播出现问题，在 SHELL 模式下输入以下命令排查：

bs /b/e iptv

cat /proc/fcache/*

cat /proc/net/igmp_snooping

cat /proc/net/ip_mr*

6.13 数据接口

ifconfig 查看网络接口（图 6-8）。

```
# ifconfig
bcmsw     Link encap:Ethernet  HWaddr B8:C7:16:08:A6:D3
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Base address:0x4200

br0       Link encap:Ethernet  HWaddr B8:C7:16:08:A6:D3
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:6774 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10264 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:639577 (624.5 KiB)  TX bytes:6781897 (6.4 MiB)

epon0     Link encap:Ethernet  HWaddr B8:C7:16:08:A6:D4
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:32227 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2179 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3554694 (3.3 MiB)  TX bytes:256071 (250.0 KiB)


epon0.0   Link encap:Ethernet  HWaddr B8:C7:16:08:A6:D4
          UP BROADCAST RUNNING PROMISC ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:81 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3860 (3.7 KiB)  TX bytes:4793 (4.6 KiB)

epon0.1   Link encap:Ethernet  HWaddr B8:C7:16:08:A6:D5
          inet addr:10.96.20.44  Bcast:10.96.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1918 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2084 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1229781 (1.1 MiB)  TX bytes:210715 (205.7 KiB)

eth0      Link encap:Ethernet  HWaddr B8:C7:16:08:A6:D3
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

图 6-8

```
veip0     Link encap:Ethernet  HWaddr B8:C7:16:21:21:21
          inet6 addr: fe80::bac7:16ff:fe21:2121/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2051830 multicast:504 unicast:63289 broadcast:1988037
          RX errors:0 dropped:3 overruns:0 frame:0
          TX packets:31494 multicast:1589 unicast:28706 broadcast:1199
          TX errors:0 dropped:0 overruns:0 carrier:0 collisions:0
          txqueuelen:0
          RX bytes:156486282 (149.2 MiB) TX bytes:6204574 (5.9 MiB)
          RX multicast bytes:27198 (26.5 KiB) TX multicast bytes:150912 (147.3 KiB)

veip0.1   Link encap:Ethernet  HWaddr B8:C7:16:21:21:24
          UP BROADCAST RUNNING MULTICAST  MTU:1492  Metric:1
          RX packets:110782 multicast:0 unicast:272 broadcast:110510
          RX errors:0 dropped:3399 overruns:0 frame:0
          TX packets:13698 multicast:0 unicast:13698 broadcast:0
          TX errors:0 dropped:0 overruns:0 carrier:0 collisions:0
          txqueuelen:0
          RX bytes:14440293 (13.7 MiB) TX bytes:4217780 (4.0 MiB)
          RX multicast bytes:0 (0.0 B) TX multicast bytes:0 (0.0 B)

veip0.2   Link encap:Ethernet  HWaddr B8:C7:16:21:21:25
          inet addr:10.96.20.29  Bcast:10.96.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:663202 multicast:0 unicast:8830 broadcast:654372
          RX errors:0 dropped:38442 overruns:0 frame:0
          TX packets:10160 multicast:0 unicast:10160 broadcast:0
          TX errors:0 dropped:0 overruns:0 carrier:0 collisions:0
          txqueuelen:0
          RX bytes:48156438 (45.9 MiB) TX bytes:1132322 (1.0 MiB)
          RX multicast bytes:0 (0.0 B) TX multicast bytes:0 (0.0 B)

veip0.3   Link encap:Ethernet  HWaddr B8:C7:16:21:21:26
          inet addr:10.96.21.36  Bcast:10.96.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:657077 multicast:0 unicast:2710 broadcast:654367
          RX errors:0 dropped:38442 overruns:0 frame:0
          TX packets:2459 multicast:0 unicast:2459 broadcast:0
```

图 6-9

epon*为 epon 型设备的 wan 侧接口，其中 epon0 为实际的网络接口，epon0.1 之类的为 vlan 虚拟网络接口

veip*为 gpon 型设备的 wan 侧接口，其中 veip0 为实际的网络接口，veip0.1 之类的为 vlan 虚拟网络接口。

eth*为 lan 侧接口 eth0、eth1、eth2、eth3 分别对应 1——4 口；eth0.0 表示 lan1 口接收和发送 untag 报文，eth0.x 接口表示 lan 侧配置 vlan 绑定功能，带 vlan 的走 eth0.x 接口。

brctl show 查看桥配置（图 6-10）。

```
# brctl show
bridge name     bridge id               STP enabled     interfaces
br0             8000.741e93cac999       no              eth2.0
                                                        eth3.0
                                                        wl0
br1             8000.741e93cac999       no              eth0.0
                                                        eth1.0
#
```

图 6-10

其中 br0，里面的接口全部绑定在 internet 属性的 wan 连接上。br1，里面的接口全部绑定在 other 属性的 wan 连接上，目前只支持 1 条 other 桥。

vlanctrl 规则，可以查看 vlan 配置的对不对，epon 规则查看（图 6-11）所示，gpon 规则查看（6-12）所示。

```
# vlanctl --if epon0 --rx --tags 1 --show-table

VLAN Rule Table : epon0, Rx, nbrOfTags 1, default DROP

--------------------------------------------------------------------------------
===> epon0 (RG) : RX, 1 tag(s)
Tag Rule ID : 1
Rx VLAN Device : epon0.1

Filters
        Tx VLANIF       : DEFAULT
        VlanDev MacAddr : Yes (ignore if multicast)
        VLAN Tag 0      : pbits -, cfi -, vid 652, (tci 0x0FFF/0x028C), ether -

Commands
        00:[POP_TAG, 0x00000000, 0x00000000]

Merge Count : 0
Hit Count   : 978

--------------------------------------------------------------------------------
===> epon0 (RG) : RX, 1 tag(s)
Tag Rule ID : 0
Rx VLAN Device : epon0.1

Filters
        Tx VLANIF       : DEFAULT
        VlanDev MacAddr : Yes

Commands
        00:[DROP_FRAME, 0x00000000, 0x00000000]

Merge Count : 0
Hit Count   : 0

--------------------------------------------------------------------------------
 81
```

图 6-11

```
# vlanctl --if veip0 --rx --tags 1 --show-table

VLAN Rule Table : veip0, Rx, nbrOfTags 1, default DROP

-------------------------------------------------------------------------------
===> veip0 (RG) : RX, 1 tag(s)
Tag Rule ID : 4
Rx VLAN Device : veip0.4

Filters
        VlanDev MacAddr : No
        Flags           : MCAST
        VLAN Tag 0      : pbits -, cfi -, vid 654, (tci 0x0FFF/0x028E), ether -
Commands
        00:[POP_TAG, 0x00000000, 0x00000000]

Hit Count    : 498

-------------------------------------------------------------------------------
===> veip0 (RG) : RX, 1 tag(s)
Tag Rule ID : 2
Rx VLAN Device : veip0.3

Filters
        VlanDev MacAddr : Yes (ignore if multicast)
        VLAN Tag 0      : pbits -, cfi -, vid 43, (tci 0x0FFF/0x002B), ether -

Commands
        00:[POP_TAG, 0x00000000, 0x00000000]

Hit Count    : 663387

-------------------------------------------------------------------------------
```

图 6-12

vlanctl --if epon0 --rx --tags 1 --show-table 查看 epon0 上接收方向，带 1 个 vlantag 的规则

vlanctl --if epon0 --tx --tags 0 --show-table 查看 epon0 上发送方向，不带 vlantag 的规则

vlanctl --if veip0 --rx --tags 1 --show-table 查看 veip0 上接收方向，带 1 个 vlantag 的规则

vlanctl --if veip0 --tx --tags 0 --show-table 查看 veip0 上发送方向，不带 vlantag 的规则

查看 igmp 相关配置，主要看 igmpproxy 和 snooping 是否启用，绑定接口是否正确

cat /var/mcpd.conf

cat /proc/net/igmp_snooping 查看 igmpsnooping 相关组

fap print 查看 fap 是否启用，有哪些规则

fap disable/enable 开关

cat /proc/fcache/* 查看 fcache 规则

fc disable/enable 开关

6.14

7 Q&A

Q：如何查看设备的 **ONU MAC** 和固件版本？

A：进入 SHELL 命令行，输入：

cat /etc/release

SVNURL:
svn://ywyysvn1.fiberhome.com.cn/project/UPONGW/src/trunk/4.14L.03_CU/bcm963xx_cu/bcm963xx

MAINVERSION: r32186

LASTCHANGE: chenyy

LASTVERSION: r32182

LSATDATE: 2013-12-10 10:36:34 +0800 (Tue, 10 Dec 2013)

BUILDDATE: 2013-12-10 13:37:27 +0800 Tue

BUILDUSER: chenyy

DESCRIPTION:

说明：目前使用的固件版本是 32182，镜像生成的时间是 2013-12-10 13:37:27 +0800 Tue

Q：如何查看设备的 **ONU MAC**？

A：进入>命令行，输入

> get base_mac

74:1e:93:d0:11:15

说明：ONU MAC = BASE MAC + 9 = 74:1e:93:d0:11:15 + 9 = 74:1e:93:d0:11:1e

Q：接上光纤后，为何有的版本 EPON 灯闪烁，有的版本 EPON 灯常亮？

A：终端硬件版本是 BCM.V2.0 版本中，EPON 等有 3 种状态，分别为常亮、熄灭、闪烁。（图 7-1）

PON 状态灯（针对 EPON 上行的设备）	绿色	网络 E	✧ 熄灭：表示 ONU 未开始注册流程； ✧ 常亮：表示 ONU 已经注册； ✧ 闪烁：表示 ONU 正在进行注册。

图 7-1

Q：升级预配置文件后，为何不能登陆 **fiberhomehg2x0** 隐藏页面？

A：部分省市预配置文件中按需求将 fiberhomehg2x0 隐藏页面用户关闭，此时需要进入 http://192.168.1.1/logoffaccount.html 界面将“隐藏用户”启用即可（图 7-2），用完后请视需求决定是否关闭该功能。

Q：为何管理员用户 **CUAdmin** 无法对 **TR069** 相关参数进行修改？

A：部分省市对管理员用户 CUAdmin 修改 TR069 相关参数进行了限制，此时需要进入 http://192.168.1.1/logoffaccount.html 界面将“Tr069 修改”启用即可，用完后请视需求决定是否关闭该功能。

Q：为何用管理员用户 **CUAdmin** 登陆会提示“当前已有用户在别处登陆，请稍后登陆”?

A：出现此提示为之前登录时异常退出导致，此时需要进入 http://192.168.1.1/logoffaccount.html 界面将“账号 CUAdmin”进行账号注销即可再次登录。

Q：设备正在注册时，为何不能再次点击“注册”按钮重复注册？

A：这是页面防止终端重复注册而做的限制，此时需要进入 http://192.168.1.1/logoffaccount.html 界面将“注册修改过程”取消即可再次进行注册。

Q：设备 **CUAdmin** 账号的密码被平台修改，如何在本地找回？

A：TELNET 上设备，进入 CLI 命令行模式，输入 dumpmdm 及可查找到 CUAdmin 账号被修改之后的密码。（图 7-2）

```
<X_BROADCOM_COM_VoiceServiceVersion>Voice</X_BROADCOM_COM_VoiceServiceVersion>
<DeviceLog>(null)</DeviceLog>
<VendorConfigFileNumberOfEntries>0</VendorConfigFileNumberOfEntries>
<X_CT-COM_MACAddress>b8:c7:16:08:a6:d4</X_CT-COM_MACAddress>
<X_CT-COM_TeleComAccount>
  <Enable>TRUE</Enable>
  <Username>telecomadmin</Username>
  <Password>nE7jA%5m</Password>
</X_CT-COM_TeleComAccount>
<X_CT-COM_MiddlewareMgt>
  <Tr069Enable>1</Tr069Enable>
  <MiddlewareURL>0.0.0.0:0</MiddlewareURL>
</X_CT-COM_MiddlewareMgt>
```

图 7-2

Q：如何在本地将设备 **result** 值置为 **1**?

A：设备默认 result 值置为 99，有可能导致本地配置 INTERNET 连接无法上网，进入 CLI 命令行模式，输入 redirect set 1 即可将设备 result 值置为 1，如需重启后仍然有效，需执行 save 命令（图 7-3）。

```
 > redirect get
99
 > redirect set 1
set successfully!
 > save
 8
backup_psi_number_blk=0 result=24576
config saved.
 >  10
```

图 7-3

Q：终端的连接无法正常获得 **IP** 地址？

A：终端无法正常获取 IP 地址需要检查 OLT 的数据：（图 7-4）

（1）OLT 上的 QINQ 域规则、QINQ 绑定

例如（在线卡上终端 WAN 连接的 MAC 地址对应的 VLAN 为 QINQ 域的外层 VLAN）：

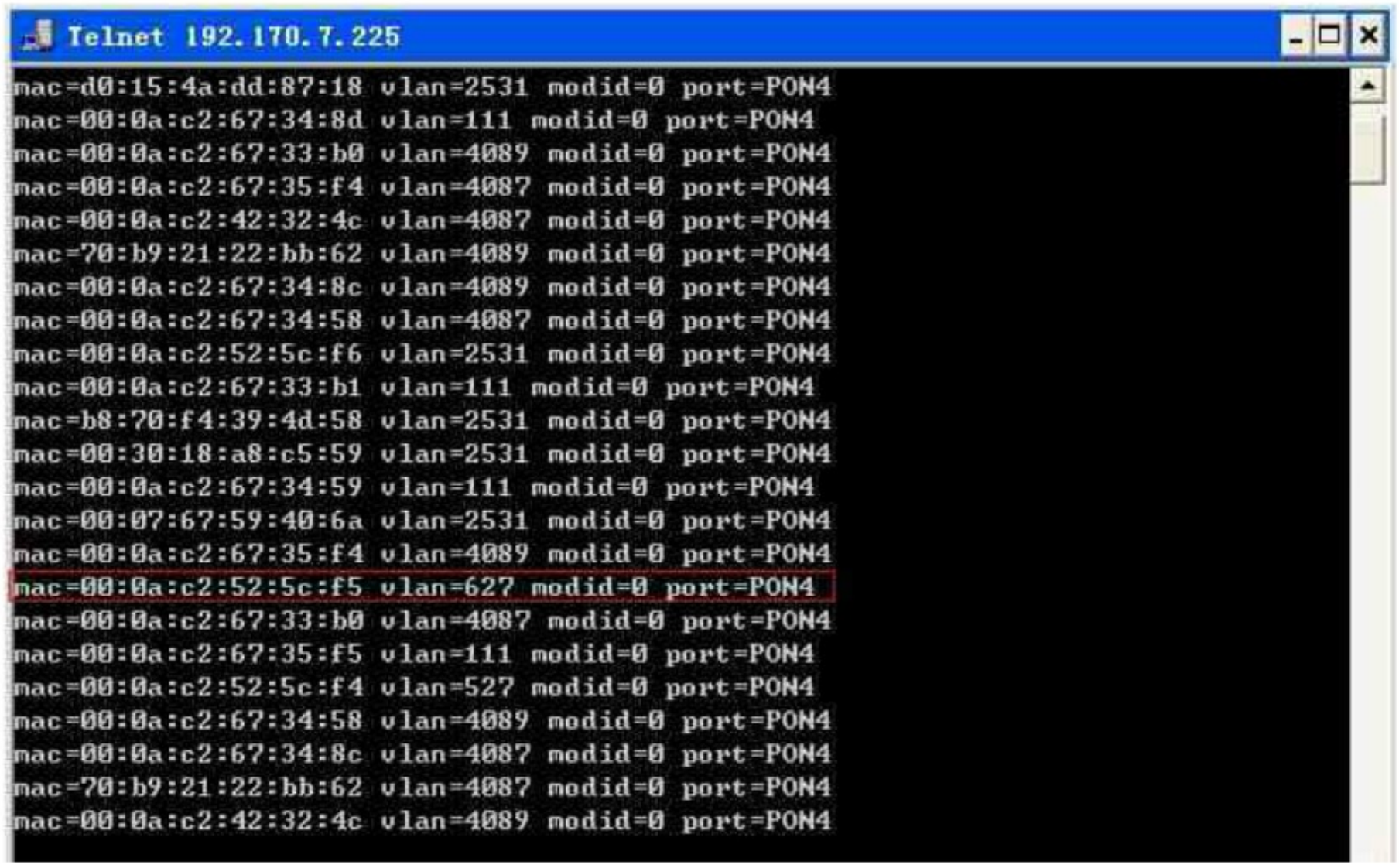

图 7-4

（2）OLT 的局端 VLAN

（3）BRAS 配置

Q：终端 **TR069** 连接获取 **IP** 地址，但是终端无法完成业务下发？

A：终端成功与 ITMS 建立通信后，终端会发送 BIND（江苏、新疆使用 BIND2）消息进行工单绑定。相关流程如下：

（1）端向 ITMS 上报 INFORM 消息，事件号至少包括： X CT-COM BIND；

（2）ITMS 收到“X CT-COM BIND”这个事件号后，通过逻辑 ID 和北向工单进行匹配；

（3）如果匹配成功，平台完成用户信息、设备信息和业务信息的绑定，下发参数 InternetGateway-Device. X_CT-COM_UserInfo.Status=0；

（4）平台在下发完业务前，下发 InternetGatewayDevice. X_CT-COM_UserInfo.Result=0；

（5）平台在下发完业务后，下发 InternetGatewayDevice. X_CT-COM_UserInfo.Result=1。

Q：终端无法正常在 **ITMS** 平台上完成工单匹配？

A：终端联通规范定义平台是否对匹配成功（status），其错误码如下：

0：成功；

1：用户认证码不存在；

2：用户逻辑 ID 不存在；

3：用户逻辑 ID 与用户认证码匹配失败；

4：超时；

5：已经注册过且无新的工单要执行；

99：缺省值，表示无认证结果信息

Q：终端无法在 **ITMS** 上完成工单下发？

A：中国联通规范规定 ITMS 平台在下发参数时，由终端侧主动发起。终端主动发起开启 TCP 窗口发送 SYN 请求，主要由以下几种：

（1）页面点击宽带账号注册，发送 BIND 消息；

（2）终端周期上报 Inform 消息，inform 消息中带有 2 PERIODIC；

（3）终端收到 ITMS 平台下发的 GET /0 HTTP/1.1。

Q：终端 Inform 中带有 0 BOOTSTRAP 事件？

A：终端 inform 中 0 BOOTSTRAPS 事件触发由以下几种情况组成：

（1）设备初次连接平台；

（2）恢复出厂设置后连接平台；

（3）修改 URL 之后连接平台；

（4）修改终端序列号之后连接平台；

Q：HG 无法实现对终端上网数的限制？

A：HG 实现终端上网数的限制的实现方法为：

（1）终端查询配置文件，读取 InternetGatewayDevice.Services. X_CT-COM_MWBAND. Mode 值，并查询多终端上网数量；

（2）查询 arp 列表，对超出多终端上网数量的 ip 地址通过 iptables 链表进行过滤。

Q：设备无法正常启动应该怎么办？

A:（1）将设备接上串口，重启设备，在启动时根据页面提示尝试回车进入 CFE 模式（图 7-5）；

```
WK01
WK01
Board IP address                  : 192.168.10.1
Host IP address                   : 192.168.1.100
Gateway IP address                :
Run from flash/host (f/h)         : f
Default host run file name        : vmlinux
Default host flash file name      : bcm963xx_fs_kernel
Boot delay (0-9 seconds)          : 1
Boot image (0=latest, 1=previous) : 0
Board Id (0-1)                    : 96828HGW
Number of MAC Addresses (1-32)    : 10
Base MAC Address                  : b8:c7:16:08:a6:d3
PSI Size (1-64) KBytes            : 24
Enable Backup PSI [0|1]           : 0
System Log Size (0-256) KBytes    : 0
Auxillary File System Size Percent: 0
Main Thread Number [0|1]          : 0
Voice Board Configuration (0-9)   : LE9530

*** Press any key to stop auto run (1 seconds) ***
Auto run second count down: 1
web info: Waiting for connection on socket 0.
CFE>
CFE>
CFE>
```

图 7-5

（2）将 PC 的地址设为静态 192.168.1.2，掩码 255.255.255.0。此时 PC 应该可以 ping 通 192.168.1.1。在 IE 上输入 192.168.1.1 进入设备串口 CFE 升级界面（图 7-6）；

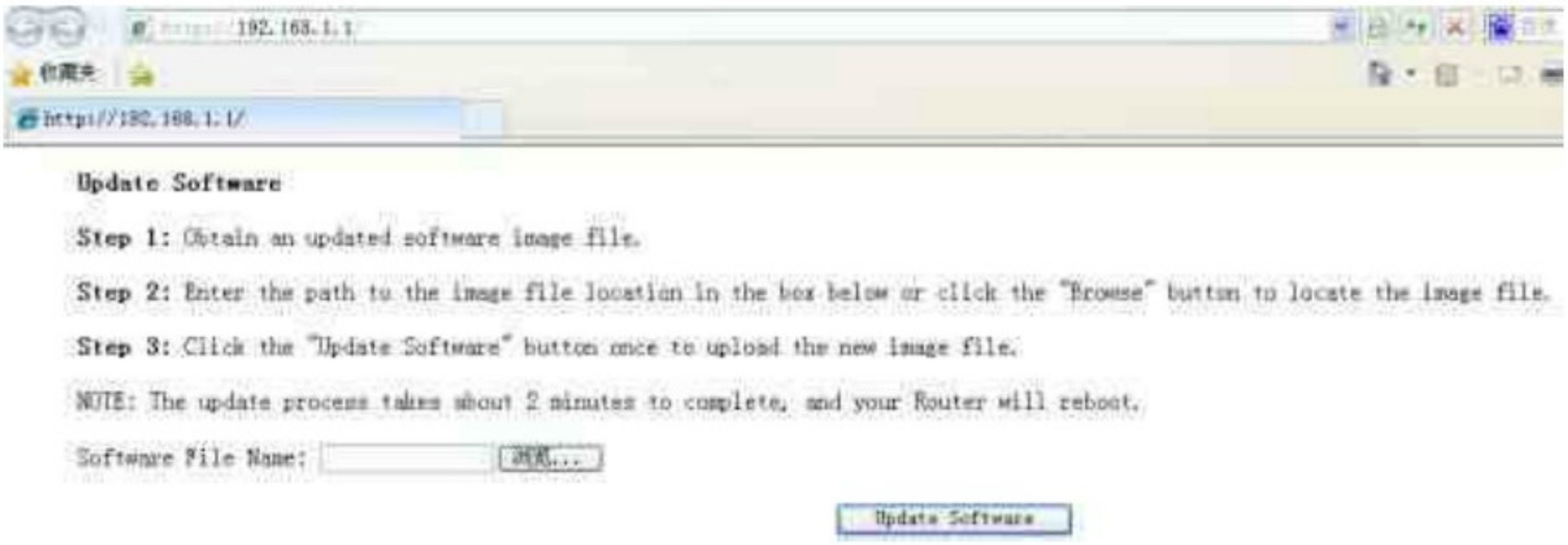

图 7-6

（3）选择带 CFE 的镜像文件（bcm96838GWOCTUPON_nand_cferom_fs_image_128_jffs2.w）升级，设备即可恢复。