安腾 eFlow

Hotel & Hotspot PnP Gateway

命令行使用手册

（版本 1.2 20060730）

广州安腾计算机网络通信技术有限公司

安腾 eFlow Hotel & Hotspot PnP Gateway 命令行手册
Part No.:
Original Issue: May. 2005

本出版物的内容将做定期性的变动，且不另行通知。更改的内容将会补充到本出版物。且会在本手册发行新版本时予以付梓印刷。本公司不做任何明示或默许担保，其中包括用户手册的内容的适应性或符合特定使用目的的默许担保。

将下列预留的空白位置，记录下序号、购买日期及机型。序号及机型可以在外盒上找到。所有与您设备元件有关的相关数据，均应包括序号、机型及购买日期。

本公司依中华人民共和国著作权法，享有及保留一切著作之专属权力，未经本公司书面同意，不得就本用户手册、改编、翻印、改造或仿制之行为。

eFlow 是广州市安腾计算机网络通信技术有限公司的注册商标。其他商标及注册商标均属于各其他所属公司。

目录

更新历史记录

更新日期	更新说明
2005-11-25	3.15，nat命令说明部分后增加set命令说明，并增加PnPGW Enterprise版本的set force_tcp_mss命令说明
2005-11-25	3.18，修改pnp smtp redirect命令说明，并增加PnPG Enterprise版本该命令的all选项说明
2005-11-25	3.18，增加非Enterprise版本的pnp http_proxy port/detect的命令说明
2005-11-25	3.27，修改session echo_interval/echo_timeout配置说明
2005-11-25	3.27，增加PnPGW Enterprise的session acct_alive命令说明，以及如何配合idle_chk和HBMS Enterprise使用
2005-11-25	3.35，增加PnPGW Enterprise的vlanuser policy/passwd_push命令说明，以及如何配合HBMS Enterprise实现高端酒店用户自选策略、公共区域漫游认证等运营特性
2005-11-25	3.39，修改webp online_win open/close的说明
2005-11-25	4.1 FAQ中，删除超长URL/cookie导致的页面异常问题，增加IE自动配置代理问题以及解决手段
2006-03-07	3.27，修改session idle_*配置使用，特别是在线小窗口与idle-timeout配合使用说明
2006-03-07	3.18，增加Enterprise版本的pnp bridge的IP地址透传配置应用说明
2006-03-07	3.36，增加Enterprise版本的vmap命令使用说明
2006-03-07	3.38，增加file.cfg和web purge的说明
2006-03-07	FAQ章节增加4.10，详细说明如何防止小窗口在线情况下发生idle-timeout
2006-03-09	删除 port enent0 的 dhcp_c 的相关配置说明
2006-03-09	3.15，增加nat list ip和nat log说明
2006-03-09	3.18，060223e版本后，默认pnp upnp disable说明
2006-04-02	3.18，pnp bridge delete <ip> 应为 pnp delete <ip>，增加pnp bridge的动态绑定说明
2006-04-02	Enterprise 060324 版本支持设置端口第二IP，3.19,增加port second_ip的说明；3.16,增加no port second_ip的说明； 3.7，增加E1 口配置second_ip的情况下DHCP地址池的特殊说明
2006-05-09	Enterprise 060422 版本合并了 pnp http_proxy port 和 session … rate 命令，非 Enterprise 的老版本不再使用，因此删除与非 Enterprise 版本有关的说明
2006-05-09	3.7，增加dhcp vlan subnet 的说明
2006-05-09	3.18，增加pnp smtp redirect的all选项过时以及如何使用nat配置完成SMTP强制转向的说明，增加了pnp http proxy detect high的副作用说明
2006-05-09	3.37，增加vpool ignore/no_ignore的说明
2006-06-12	3.15， nat配置增加SMTP强制转发以及nat show的相关说明，set配置增加了防P2P下载set deny_bt，以及与MAC安全策略相关的set black_mac/black_mac_threshold的说明
2006-06-12	3.27，增加防垃圾邮件session spam_threshold配置说明
2006-06-12	3.28，增加show deny_bt/spam/black_mac说明
2006-06-12	3.29，更新show session <ip> 的详细说明
2006-06-12	FAQ章节4.8，说明无portal模式下的代理发现条件和配置注意
2006-06-12	更新附录5.1章节RADIUS属性列表
2006-07-30	3.15， nat配置增加未认证用户POP邮件帮助说明，set配置增加set black_mac_timeout，已经黑名单例外的说明
2006-07-30	3.18，增加pnp netbios enable|disable的说明
2006-07-30	3.28，增加show system和show bwstat说明，3.29，增加show session_pass的说明
2006-07-30	增加FAQ章节4.11，说明如何定制用户上网帮助邮件

一、 总述

安腾 eFlow Hotel & Hotspot PnP Gateway（以下简称 PnPGW）可广泛应用于商务人士较集中的商务酒店以及机场、咖啡吧等 WLAN 热点覆盖区域等，为需要宽带服务的商务人士提供宽带上网服务。PnPGW 内置了强大的安腾 eFlow PnP 引擎，用户电脑不需做任何 IP 设置改动，就可以接入到 PnPGW 享受快捷的上网服务，同时也大大降低了酒店/运营商的维护成本。

PnPGW 可以单独部署于运营点出口为用户提供上网服务，也可以与外部 RADIUS 配合实现用户认证和计费。如下图 1-1 所示， PnPGW 与安腾 eFlow Hotel AAA 酒店宽带管理和计费软件配合，可实现一个高可靠性、高可管理性的酒店宽带运营解决方案。

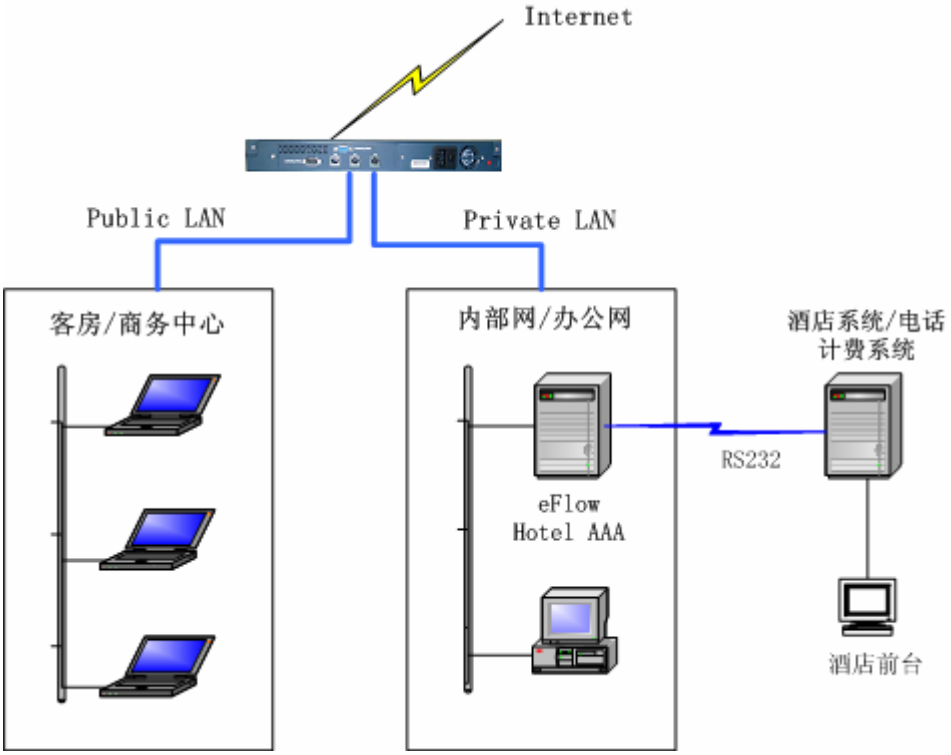

图 1-1

1.1 设备外观

PnPGW 前视外观见下图，有电源指示灯、FLASH 指示灯和三组网络端口状态指示灯：

图 1-2

PnPGW 的后面板有一个 220V 交流电源插口及开关、3 个 10/100M 自适应的 RJ45 端口和两个 RS 232 的 CONSOLE/PMS 口。三个 RJ45 端口包括一个 WAN 端口，编号为 E0，作为上行链路端口；一个 Public 端口，编号为 E1，作为用户接入/认证端口；

一个 Private 端口，编号为 E2，可作为网管或者内部办公网专用端口。RJ45 口上方的 CONSOLE 口可使用 WINDOWS 超级终端的默认参数连接，即波特率 9600，8 个数据位，无校验，1 个停止位，硬件流控或者 Xon/Xoff。用户可以使用超级终端连接到 PnPGW，进行命令行方式的配置和各种系统运行状态参数的查看。RJ45 口左方的 RS232 口为 PMS 扩展端口，目前不用。右下角的红色按纽为设备复位（RESET）按纽。PnPGW 的后面板见下图 1-2：

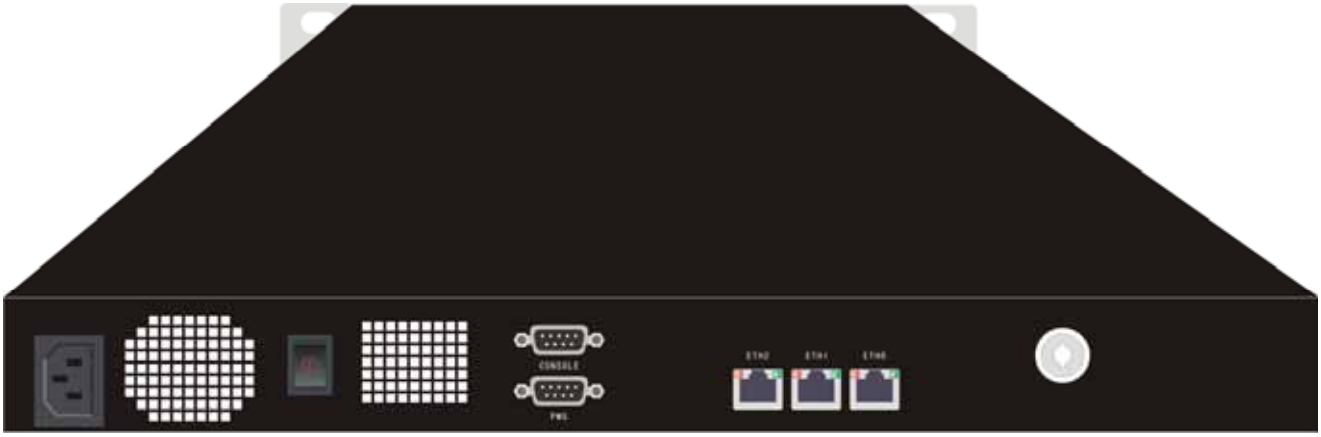

图 1-3

1.2 硬件规范

PnPGW 的硬件规范如下表：

处理器和内存	物理接口
PENTIUM III，128M RAM	3 个 10/100M 以太接口
电源	功率
220V 交流电源	300 瓦
外观尺寸	重量
43cm×34cm×5cm	4 公斤
工作环境	
温度： 摄氏 0–50 度	相对湿度：5-90%

表 1-1

1.3 功能特性

PnPGW 是一款主要面向二层接入环境的宽带接入服务器设备（若跨三层则无法使用 PnP），最大支持并发 512 用户。具有强大的网络和用户接入/控制功能。PnPGW 的主要功能特性见下表：

网络功能	IP 静态路由
	NAT（包括动态、静态）和 ACL
	WAN 端口 PPPoE 拨号支持
	DHCP Server 和 DHCP Relay
	PROXY ARP
	LAN 口支持 802.1Q VLAN，最大 4094VLAN
接入和控制功能	WEB 认证
	VLAN 认证
	IP PNP 服务
	DNS/HTTP 代理/SMTP 强制转向
	强制转向 URL
	在线用户 Keep-Alive，包括 WEB 或者单播 ARP 两种方式
	Idel-Timeout 检测支持
	用户带宽限制，粒度为 32kbps
	用户最大 NAT Session 数限制
	IP/MAC 绑定
	RADIUS CLIENT，可由 RADIUS 授权控制用户的带宽、首页 URL
管理特性	TELNET 和 CONSOLE 口的命令行方式管理
	WEB 管理
	TFTP 软件升级
	SNMP AGENT 支持

表 1-2

二、 初步安装及配置

2.1 设备安装

在安装之前，确认电源开关为未打开。设备本身附带有上架配件，按照标准程序把设备固定在机架上；

将 PnPGW 的 E0 口（WAN）与出口链路连接正确；

将 PnPGW 的 E1 口（Public）与汇聚交换机连接正确；

将 PnPGW 的 E2 口（Private）与管理计算机 CONSOLE 口相连，也可通过交换机或直接使用交叉线进行网络连接；

将 PnPGW 与电源连接加电；

2.2 初步配置和管理

管理计算机的串口设置为 9600，8N1 进行连接，回车后即显示 Login 的提示，初始用户名为 amtium，密码为 eflow，命令 enable 即可进入到配置模式，enable 的初始密码为 eflow。用户也可以用 telnet 进行命令行配置，PnPGW 的 E2 端口出厂默认配置为 172.31.14.1，管理计算机可配置 IP 地址为 172.31.14.0/24 子网段的其它 IP 地址，比如 172.31.14.2，telnet 172.31.13.1 即可登录到 PnPGW 进行命令行配置。

对于首次配置，建议进入到 WEB 管理管理界面使用快速配置功能生成初步的配置，之后再使用命令行或者继续使用 WEB 方式进行细化的配置。WEB 方式的具体配置过程详细见 PNPGW 的 WEB 管理手册。

2.3 配置分类及概貌

2.3.1 配置分类指引

1. 端口和路由

PnPGW 首要的配置就是端口和路由配置，以保证内外网的连通性。E0 端口的模式有最常用静态 IP、以及 PPPoE 拨号，当配置 E0 口为静态 IP 时，必须指定上级默认路由。可参考 port、pppoe_c 和 route 命令的详解。

E1 和 E2 端口为内网端口，其中 E1 一般处于接入模式，E2 作为内部办公网或者专用网管口，处于普通路由模式。接入模式对用户具有更强的管理和控制功能，包括控制用户的上下行带宽、NAT 会话数等等，当 E2 下内部办公网环境比较复杂比如用户中病毒情况比较多，也建议在 E2 上启用接入模式。注意如果 E1 和 E2 都启用了接入模式，那么一定不能在组网上将 E1 和 E2 部署在同一广播域中。将端口模式设置为接入模式的配置为 dhcp enet1/2 input，可参考 dhcp 命令详解。

除了端口和路由，另外一个和系统服务相关的就是 DNS 配置，不配置正确的 DNS，将导致用户上网异常现象，比如网页打不开、email 发送/接收不了等。建议使用本地运营商最可靠的主和备用 DNS。可参考 nameserver 命令详解。

2. 系统服务

系统服务包括 DHCP 服务和 WEB Portal。DHCP 服务为接入用户分配 IP 地址，而 WEB Portal 则可灵活配置认证用户的认证页面、实现 VLAN 认证、控制是否转向 URL、转向到哪个 URL 等等。可参考 dhcp 和 webp 命令详解。

3. 认证用户管理

认证用户管理可配置实现哪段地址进行 Web 认证、哪段地址为专线用户不需要认证，以及指定用户的带宽、NAT 会话等资源。可参考 session 命令详解。

4. PNP 服务

PNP 服务可使得 E1 端口下的用户即使配置了其它子网段的静态 IP 地址也能正常接入到 PnPGW。即使对一些较复杂用户配置情况，PNP 服务也能保证用户接入正常，比如用户配置了错误的 DNS，或者配置了 HTTP Proxy，或者地址与 E1 同子网段但是网关并没有指向 E1 的 IP 地址。可参考 pnp 命令详解。

5. NAT 和 ACL

PnPGW 具有 NAT 功能，使得内网用户可共享出口 IP 访问外网，并可实现外网可访问内网的网管资源。PnPGW 的 ACL 功能可配合网管人员过滤掉不希望转发的流量，优化网络环境，增强网络安全。可参考 nat 和 filist 命令详解。

6. Radius Client

PnPGW 可与 Radius Server 配合实现用户认证/计费。可参考 radius 命令详解。

7. 其它管理功能

PnPGW 提供了一些命令行接口帮助管理员查看系统状态，并提供了其它一些命令增强系统可管理性。比如 show 系列命令可查看系统资源，snmp 命令可配置系统的网管，arp 命令可实现对重要主机进行 ARP 绑定防止被抢 IP，backup/upgrade 和 cfg 命令可备份/升级系统 IOS 以及备份/更新系统配置。

2.3.2 快速配置示例

以下是一个快速配置生成的配置示例，用于不计费认证的场合（当需要认证计费时，只需要 pnp pass disable，并配置正确的 radius 指向即可），可以以此初步了解 PnPGW 的配置概貌：

```
! 配置 E0 地址为 192.168.14.123，E1 口 172.31.13.1，E2 口 172.31.14.1
port enet0 ethernet   192.168.14.123   255.255.255.0
port enet1 ethernet   172.31.13.1   255.255.255.0
port enet2 ethernet   172.31.14.1   255.255.255.0
! 配置主备 DNS Server 的地址
nameserver primary 202.96.209.5
nameserver secondary 202.96.199.133
! 配置 IP PNP，为不认证计费模式
pnp enable
pnp dns redirect
pnp http_proxy redirect 172.31.13.1 8080
pnp pass enable
pnp no_arp_pub disable
! 配置 E1 口的 DHCP 和分配地址段
dhcp enet1 input
dhcp lease 60
dhcp server enable
dhcp address 172.31.13.2 253 255.255.255.0 172.31.13.1
```

```
dhcp umac disable
! 配置认证地址段以及认证用户管理和控制相关的参数
session address 172.31.13.2 253
session echo_timeout  180
session echo_interval 90
session acct_interval 0
session idle_chk disable
session idle_data 1
session idle_timeout 30
session max_nat_num 130
session web_num 25
session admin enable
! 配置 WEB Portal
webp url http://www.amtium.com
webp redirect_url disable
webp online_win open
webp vlan_page disable
! 本地帐号
user name amtium passwd eflow
! 允许本地认证
local auth enable
! 默认路由为 192.168.14.1
route add 0.0.0.0 0.0.0.0 192.168.14.1
! 配置 NAT
nat add map enet0 172.31.13.0/24 192.168.14.123/32 portmap
nat add map enet0 172.31.13.0/24 192.168.14.123/32
nat add map enet0 172.31.14.0/24 192.168.14.123/32 portmap
nat add map enet0 172.31.14.0/24 192.168.14.123/32
!
nat no_auto
! 配置 IP 包过滤规则
filist add enet1 block in tcp 0.0.0.0/0 0.0.0.0/0 dstport = 135 quick
filist add enet1 block in tcp 0.0.0.0/0 0.0.0.0/0 dstport = 139 quick
filist add enet1 block in tcp 0.0.0.0/0 0.0.0.0/0 dstport = 445 quick
filist add enet1 pass in icmp 0.0.0.0/0 172.31.13.1/32 quick
filist add enet1 block in icmp 0.0.0.0/0 0.0.0.0/0 quick
! 不启用组播路由
multi off
! 配置宽带服务名
servicename internet
! 配置主机名
hostname pnpgw
! 配置 WEB 认证类型
auth pap
! 配置网管和 NAT 超时参数
```

```
snmp com default r
snmp trap 0.0.0.0
snmp trap_version 1
set nat_tcptimeout   300
set nat_udptimeout   60
set nat_icmptimeout  60
!
```

三、 命令详解

PnPGW 的命令行有两种模式，一是简单的设备状态查看模式，用户登录到设备即进入此模式，命令行提示符为>，此时只能使用有限的命令行进行一些基本的设备状态查看。当用户敲入 enable 命令并认证通过时候，及进入到设备配置模式，此时命令行提示符为#，用户可以修改设备配置，并可以进行一些更高级的设备状态查看，比如使用 debug 命令。

所有命令的用法都可以用命令加 ? 参数来进行查看，比如 show ?，port ? 等等。命令行由关键字和参数组成，可有多个关键字或参数，/或|字符表示关键字或参数可选其一，[]表示可选的命令行参数，<>表示必选的命令行参数。

3.1 ?

用法：?

说明：

显示当前命令行模式的可用命令

例如在设备状态查看模式下显示了可用的几个命令以及简单说明:

```
> ?
pnpgw> ?
show                show system information
ping                test network
enable              get full right
time                display or set system time
exit                quit current shell
?                   show help
```

3.2 arp

用法:

```
arp bind <ip> <mac>
arp unbind/query/del <ip>
arp show
```

说明：

该命令进行 ARP 表的操作,包括 arp 绑定/解除绑定/查询/手工删除。arp bind 添加一个静态绑定的 arp 表项,arp unbind 删除一个静态绑定表项，arp del 删除当前 arp 表中的一个表项。注意 arp del 和 arp unbind 的不同，arp del 只是删除 ARP 表项，而不影响 bind 配置，bind 配置在设备 reboot 后仍然生效，而 arp unbind 两者都影响，即删除 ARP 表项，又删除配置中的绑定关系。注意 mac 地址的格式，是严格的 xx:xx:xx:xx:xx:xx，其中 x 是不区分大小写的 16 进制字符。在实际运营环境中，通常需要对一些重要的主机（比如 Radius Server 或者酒店前台 PC 部署在 E1 同段内）进行 arp 绑定，避免在 IP 冲突或者被恶意抢占时，影响重要主机和 PnPGW 之间的通信。

例如：

```
# arp bind 172.16.0.8 00:40:b8:00:57:86
```

配置 ip 为 172.16.0.8 与 mac 为 00:40:b8:00:57:86 绑定。

arp unbind 172.16.0.8

解除 ip 为 172.16.0.8 ARP 表项绑定关系。

arp del 172.16.0.8

手工删除 ARP 表中 IP 为 172.16.0.8 的表项。

arp query 172.16.0.8

查询 IP 地址为 172.16.0.8 的 ARP 表项。

arp show

LINK LEVEL ARP TABLE

destination	gateway	flags	Refcnt	Use	Interface
192.168.14.110	00:01:02:9a:1a:c9	c05	0	3	el1
192.168.14.111	00:02:b3:35:82:95	c05	0	0	el1
192.168.14.112	00:50:10:21:59:70	c05	0	0	el1
192.168.14.123	00:d0:c9:95:64:3a	405	0	3	el1

以上显示系统当前的 ARP 表信息。注意 flags 列，c05 表示静态的不可动态刷新的 ARP 表项，只能通过 arp del 或 arp unbind 命令删除；而 405 则是一般的可动态刷新的 ARP 表项，当主机长时间不活动时，表项将超时被系统删除，超时时长为 20 分钟。

3.3 auth

用法：auth chap/pap

说明：定义系统 WEB 认证类型为 CHAP 还是 PAP，其中 CHAP 对密码进行加密，而 PAP 则是明文传输密码。通常使用 auth pap 的配置即可。

例如：

auth pap

定义 pap 认证类型。

auth chap

定义 chap 认证类型。

3.4 backup

用法：backup

说明：备份系统 IOS。

例如:

backup

备份系统 ios。注意系统一般在系统升级前需要做 backup，而系统刚升级完毕时，backup 命令将被禁止运行。

3.5 cfg

用法：cfg put|get <tftp_server> <filename>

说明：从 tftp 服务器获取或保存配置文件。

例如:

cfg get 192.168.1.2 pnpgw.cfg

从 tftp 服务器(地址为 192.168.1.2)中获取名字为 pnpgw.cfg 的文件作为系统的配置文件，注意要在系统 reboot 重启动后新的配置才生效。

cfg put 192.168.1.2 pnpgw.cfg

把当前的配置文件保存在地址为 192.168.1.2 的 tftp 服务器上。

3.6 debug

用法：

debug radius/pnp_htproxy on/off

debug dhcp/dhcp_bind

debug show

说明：配置调试开关，以便在系统 console 口上观察所需要的系统调试信息。debug radius on 可以观察到设备 radius client 和 radius server 之间的通信行为，debug pnp_htproxy on 可以观察到配置了 http 代理的用户认证行为。debug dhcp 可以观察当前被 DHCP Server 分配的 IP 地址数，dhcp dhcp_bind 可以观察当前被 DHCP server 分配的 IP/MAC 地址绑定项目。注意 debug ... on 进行调试以后，需要再 debug ... off 关闭调试开关，过多地在 console 口上显示调试信息将影响系统性能。

例如:

debug radius on

打开 RADIUS 调试开关。

debug show

显示各调试开关的当前状态。

3.7 dhcp

用法：

dhcp server enable|disable

dhcp enet[1/2/3] input

dhcp address <begin_ip> <num> <mask> <route>

dhcp relay <ip> <network>

dhcp lease <minute>

dhcp vlan <vlan_id> subnet <network>

dhcp agent <server_ip>

dhcp umac enable/disable

dhcp umac list

dhcp umac get|put <tftp_server> <filename>

说明：

配置 DHCP Server、地址段和 DHCP AGENT 功能

dhcp server enable|disable 开启/关闭 dhcp 服务器，如果要使用 dhcp agent 功能应关闭 dhcp 服务器(disable)

dhcp enet[1/2/3] input 表示允许端口接收 DHCP 请求，并设置端口模式为接入端口，而不是路由端口。默认配置 dhcp enet1 input，则 E1 口总是作为接入端口，允许接受 DHCP 请求，某些情况下可能需要将 E2 端口也配置为接入端口，改变端口模式时，需要重新启动 PnPGW。若要关闭端口的 DHCP 和接入功能，可使用命令 no dhcp[1/2/3] input。

dhcp address <begin_ip> <num> <mask> <route>

配置 dhcp 地址池，例如：

dhcp address 10.1.1.2 253 255.255.255.0 10.1.1.1

配置从 10.1.1.2 开始的 253 个 IP 地址可供 dhcp 分配，掩码是 255.255.255.0 （注意掩码和接入端口的子网掩码的匹配），以 10.1.1.1 作为缺省网关(一般此时接入端口的 IP 地址就设成 10.1.1.1)

可以用 dhcp address 命令配置多个地址池，配置时注意各接入端口 IP 子网与各地址池的 IP 子网的匹配。特殊情况下，当 E1 口配置了 second_ip 后，可以为 E1 口的 second_ip 所属的子网也指定一个地址池。若 E1 口拥有分属两个不同子网的地址池时，当 DHCP 请求到达 E1 口时，DHCP Server 总是尝试先从与 E1 口第一个 IP 子网匹配的地址池中先分配地址，当分配失败时，再尝试从与 second_ip 子网匹配的地址池中分配地址，这样可以实现一些特殊 DHCP 配置要求，比如先分配公网再分配私网地址。特别注意，E1/2 端口都可配置 second_ip，但只有 E1 口可有效配置与 second_ip 子网匹配的 DHCP 地址池。

PnPGW Enterprise 20060422 版本增加了 dhcp vlan <vlan_id> subnet <network>命令，可以为特殊 VLAN 指定 DHCP 分配的子网。典型应用在 E1 口先分配公网再分配私网、办公网和客房网 VLAN 隔离但是同位于 E1 的情况下，此时希望办公网用户拿到私网 IP 地址以节省公网地址。注意 network 参数必须为严格的子网号，且与端口子网地址匹配，注意仅当 E1 配置了 session_ip 时该配置才有效。目前该配置为单条配置，不支持为多个 VLAN 或者 VLAN 范围指定分配子网，因此组网时要求办公用户位于同一 VLAN 下，而不是分布于多个 VLAN。典型配置如下，为办公 VLAN 180 分配私网地址：

dhcp address 222.66.89.194 29 255.255.255.224 222.66.89.193

dhcp address 10.0.228.2 400 255.255.254.0 10.0.228.1

dhcp vlan 180 subnet 10.0.228.0

dhcp relay <ip> <network>

配置本服务器接收并处理来自其他设备的 dhcp 中继包分配 IP 地址，其中<ip>是发送 dhcp relay 包的设备 IP。

dhcp lease <minute>

配置 IP 地址的分配时长，单位为分钟。默认 60 分钟。

dhcp agent <server ip>

把本服务器作为 DHCP 中继设备，本身不分配地址而将分配地址的请求发送到<server ip>的设备上。要使用本功能应将 dhcp server 功能关闭。

dhcp umac enable/disable

启用或关闭按 MAC 地址固定分配 IP 地址的功能。

dhcp umac list

列出当前按 MAC 地址固定分配 IP 地址的对应列表

dhcp umac get|put <tftp_server> <filename>

使用 tftp 从指定的 tftp server 获取或者保存当前的 MAC/IP 分配列表文件。MAC/IP 分配列表文件的格式为每行为一个 MAC/IP 地址分配对应关系，包含四列，第一列为 MAC 地址，第二列为 IP 地址，第三列为掩码，第四列为默认网关。MAC 地址的格式为 XXXXXXXXXXXX，即 12 位 16 进制字符，举例如下：

```
# Mac_Address   U_IP        U_Mask          U_Route
0010605b1958    10.1.1.7    255.255.255.0   10.1.1.1
0001e24fca9c    10.1.1.4    255.255.255.0   10.1.1.1
```

注意配置文件的 IP 不能同 dhcp address 配置的地址有重叠。

比如按照如上的文件格式做一个 UNIX 格式的文本文件（注意不能是 DOS 格式的）umac.cfg ，将用户的 MAC 和要绑定的 IP 地址、掩码、网关都写进去。然后通过地址为 192.168.0.139 的 tftp 服务器，将 umac.cfg 传到 PnPGW 里。

dhcp umac get 192.168.0.139 umac.cfg

dhcp umac enable

保存配置重启后配置生效。

3.8 enable

用法：

enable

enable password

说明：在系统状态查看模式下，enable 命令用于进入到配置模式。在配置模式下，enable password 命令用户修改 enable 的密码。修改 enable 密码需要先输入旧的 enable 密码，再输入和确认新的 enable 密码。

3.9 exit

用法：exit

说明：退出配置模式或者推出命令行

3.10 filist

用法：

filist add/del <port> block/pass in/out <protocol> <src_ip_pool> [srcport <scmp> <port>] <dst_ip_pool> [dstport <dcmp> <port>] [quick]

filist flush/list

说明：配置和查看 IP 过滤规则列表，add/del 添加或删除规则，flush 清空所有规则，list 查看当前规则列表。

规则关键字和参数说明：

port	端口参数，可以是 enet0/1/2
block/pass	匹配行为关键字，当规则匹配，阻断还是允许报文通过
in/out	IP 报文方向关键字，相对与设备端口来说，是流入还是流出
protocol	协议参数，可以是 icmp/udp/tcp
src_ip_pool	源 IP 地址匹配参数，格式为 ip/prefix，其中 ip 为子网段 ip 地址，prefix 为子网段的掩码位数 当匹配单个 IP 地址时候，写为 ip/32，比如 10.1.1.2/32，当匹配所有 IP 地址时，写为 0.0.0.0/0
dst_ip_pool	目的 IP 地址匹配参数，格式同 src_ip_pool
srcport scmp port	可选的 TCP/UDP 源端口匹配表达式，srcport 为关键字，scmp 参数可以是'>' '<' '>=' '<=' '='，port 是 TCP/UDP 端口，比如 srcport = 20
srcport scmp port	可选的 TCP/UDP 目的端口匹配表达式，dstport 为关键字，scmp 参数可以是'>' '<' '>=' '<=' '='，port 是 TCP/UDP 端口，比如 dstport = 8080
quick	可选的匹配行为关键字，指定 quick 的过滤规则表示，若该规则匹配，则直接按规则 block 或 pass，而不再进行后续规则的匹配查找

例如：

filist flush

清除所包过滤规则。

filist list

显示所有过滤规则。

filist add enet0 block in tcp 0.0.0.0/0 192.168.1.168/32 dstport = 23 quick

在端口 enet0 阻断所有目的地址为 192.168.1.168 的 telnet 请求报文。

以下是 PnPGW 的 WEB 管理快速配置后生成的针对接入端口 E1 的默认过滤规则，假设 E1 的 IP 地址为 172.31.13.1，掩码为 255.255.255.0：

```
# filist add enet1 block in tcp 0.0.0.0/0 0.0.0.0/0 dstport = 135 quick
# filist add enet1 block in tcp 0.0.0.0/0 0.0.0.0/0 dstport = 139 quick
# filist add enet1 block in tcp 0.0.0.0/0 0.0.0.0/0 dstport = 445 quick
# filist add enet1 pass in icmp 0.0.0.0/0 172.31.13.1/32 quick
# filist add enet1 block in icmp 0.0.0.0/0 0.0.0.0/0 quick
```

上述规则中，前三条过滤了 NetBIOS 相关的流量，可以一定程度上防止利用了微软 NetBIOS 漏洞的蠕虫病毒进行进一步传播；后两条规则则允许用户发送目的地址为 E1 口 IP 的 ICMP 报文，而其它的 ICMP 报文则全部丢弃不进行转发，这样做的直观效果就是在 E1 口范围内，允许接入用户 ping PnPGW 的 E1 口，也允许从 PnPGW ping 处于 E1 口的接入用户（注意 PnPGW 的 DHCP Server 有时需要主动 ping 用户以探测 IP 是否可分配），其它条件的 ping 则全部失败。

PnPGW 具有 WEB 管理功能，建议在正式运营后，禁止从公网访问 WEB 管理（端口为 TCP 81），以保护 PnPGW 的 WEB Server 不被恶意用户从公网进行 DoS 攻击而影响正常使用，比如 E0 口 IP 地址为 202.99.131.2，那么可以追加下面一条过滤规则：

filist add enet0 block in tcp 0.0.0.0/0 202.99.131.2/32 dstport = 81 quick

3.11 hostname

用法：hostname <name>

说明：配置主机名

例如:

hostname pnpgw

定义主机名为 pnpgw。

3.12 local

用法： local auth enable/disable

说明： 配置是否允许进行本地帐号认证，即 user 命令配置。PnPGW 的认证行为是，若允许本地认证，则先先查询本地帐号，若本地帐号不存在而又允许 Radius 认证，再通过 Radius client 来发送认证请求到 Radius Server。

例如:

> local auth enable

允许本地认证。

3.13 multi

用法：multi on/off/show

说明：配置组播（multicast）路由。multi on/off 启用或关闭组播路由。multi show 查看当前的组播路由配置。若运营环境中有经过 PnPGW 转发的组播业务流，则配置为 multi on。默认配置为 multi off。

3.14 nameserver

用法：nameserver primary/secondary <ip>

作用：配置首选和备用域名解析服务器服务器的 IP 地址，该配置作为 DHCP Server 为用户分配的 IP 地址，prmary DNS 同时还作为 PNP 用户的强制转向 DNS，因此要求使用本地运营商最可靠的 DNS 服务器。

例如:

nameserver primary 192.168.1.2

把首选域名服务器指向地址 192.168.1.2

nameserver secondary 192.168.1.88

把备用域名服务器指向地址 192.168.1.88

3.15 nat/set

用法：

nat add/del map/rdr <port> <src_ip_pool> [srcport <port>] <map_ip_pool> [dstport <port>] [portmap]

nat list [ip]

nat flush/auto/no_auto/auto_show/show

nat log <log_server_ip> <log_server_port>

nat log disable

nat show

说明：nat add/del 添加或删除 NAT 规则，nat list 列出当前规则以及 NAT 统计信息，nat flush 删除所有规则。nat auto 命令只使用在 E0 口配置成 pppoe client 或者 dhcp client 的情况（参考 port enet0 dhcp_c|dhcp_c），这两种情况的配置下，出口地址是可以动态改变的，当出口地址改变时，nat auto 会自动调整所有和出口 IP 相关的 NAT 规则，包括 map 和 rdr 规则。nat no_auto 关闭自动调整 NAT 规则功能，nat autoshow 查看当前是否启用 NAT 自动调整规则功能。

NAT 规则的关键字和参数说明：

port	端口参数，可以是 enet0/1/2，一般为 enet0，一般来说，NAT 规则总是配置在出口上。
map/rdr	NAT 行为关键字，map 是对 IP 报问的源 IP/端口进行转换，rdr 是则是对目的 IP/端口进行转换
src_ip_pool	被转换的 IP 地址匹配参数，格式为 ip/prefix，其中 ip 为子网段 ip 地址，prefix 为子网段的掩码位数。注意当为 map 规则时候，指 IP 源地址信息，当为 rdr 规则时候，指 IP 目的地址信息。当匹配单个 IP 地址时候，写为 ip/32，比如 10.1.1.2/32。
srcport port	可选的被转换 TCP/UDP 端口表达式，srcport 为关键字，port 为 TCP/UDP 端口参数。注意当为 map 规则时候，指源端口地址信息，当为 rdr 规则时候，指目的端口信息。
map_ip_pool	转换 IP 地址，格式同样为 ip/prefix。
srcport port	可选的转换 TCP/UDP 端口表达式，dstport 为关键字，port 为 TCP/UDP 端口参数。
portmap	可选 NAT 行为关键字，只用于 map 规则，表示是否做 NAPT，即做 IP 地址转换的同时，又进行端口转换。

例如 PnPGW 的 E0 配置为 202.96.196.32/255.255.255.240，E1 地址为 10.1.1.1/255.255.255.0:

```
# nat add map enet0 10.1.1.0/24 202.96.196.32/32 portmap
# nat add map enet0 10.1.1.0/24 202.96.196.32/32
```

在 enet0 口上，将源头地址为 10.1.1.0 到 10.1.1.255 的地址转换为 202.96.196.32 的出口地址上，有 portmap 的行指定进行端口转换，没有 portmap 的行针对非 tcp/udp 类进行 IP 转换。

可使用 nat rdr 配置完成 SMTP 强制转向配置，使得 E1 口下所有用户的 SMTP 请求被透明转发到指定的外部 SMTP 服务器进行处理，比如外部 SMTP 服务器地址为 218.1.4.36：

```
nat add rdr enet1 0.0.0.0/0 srcport 25 218.1.4.36/32 dstport 25
```

PnPGW 3.3 以后版本中，可使用 nat rdr 配置完成对未认证用户的 MAIL 帮助，此配置将使得 E1 口下未认证用户尝试 POP3 收取 mail 时，将收到系统预先定制的上网帮助邮件，比如 E1 口为 172.31.13.1：

```
nat add rdr enet1 0.0.0.0/0 srcport 110 172.31.31.1/32 dstport 110
```

如何定制帮助邮件见 FAQ 4.11。

```
# nat add enet0 rdr 202.96.196.32/32 srcport 22 10.1.1.254/22 dstport 22
```

将 202.96.196.32 的 ssh 连接请求转向到内网的 10.1.1.254,使的外部用户能够通过 ssh 连接到内部主机进行远程管理。

```
# nat add rdr enet0 202.96.196.33/32 10.1.1.253/32
# nat add map enet0 10.1.1.253/32 202.96.196.33/32
# proxyarp add 202.96.196.33 255.255.255.0
```

上面配置例子中，两条 NAT 规则将公网络地址 202.96.196.33 静态映射为内部地址 10.1.1.253，由于 202.96.196.33 包含在 E0 所属的子网段内，因此配置 proxyarp 可通告该子网其它主机将目的地址为 202.96.196.33 的 IP 报文发到 PnPGW 的 E0 口。详细见 proxyarp 配置说明。

```
# nat del map enet0 10.1.1.0/24 202.96.196.32/32
```

删除 enet0 口的一条 NAT 规则。

```
# nat list [ip]
```

显示所有当前 NAT 规则，前 100 个活动 NAT 会话，以及 NAT 会话数统计。当带有 ip 参数时，显示源或者目的地址与 ip 参数匹配的 NAT 会话，一般可以用来显示某用户的活动 NAT 会话，最大显示 500 条。

```
# nat flush
```

删除所有 NAT 规则配置和 NAT 会话。

```
# nat show
```

显示当前的 NAT 规则配置。当配置了 SMTP 强制转发时，系统会自动定时探测转向目的 SMTP 服务是否可达，nat show 将显示转向目的 SMTP 服务是否可达，当不可达时，系统自动禁用 SMTP 强制转向，直到系统再次探测服务可达时才恢复 SMTP 强制转向功能。

PnPGW 支持 NAT 会话日志，nat log <log_server_ip> <log_server_port> 可配置日志服务器的 IP 地址和 UDP 服务端口，向指定 IP 和端口的日志服务器发送用户上网会话日志。一般来说上网日志服务软件包可安装在计费服务器上，日志服务器的默认服务端口为 UDP 1813，也可以改配其它端口，详细见 NAT 日志服务器软件安装说明。nat log disable 关闭 PnPGW 的日志记录功能。

与 NAT 超时参数相关的 set 命令用法如下：

set nat_tcptimeout <sec>

set nat_udptimeout <sec>

set nat_icmptimeout <sec>

上述命令分别配置 TCP/UDP/ICMP 的 NAT session 的 IDLE 超时时长，一般了来说，使用默认参数即可。

PnPGW Enterprise 版本另外还支持 set force_tcp_mss <bytes>命令，强制改变用户 TCP 流的 TCP MSS 选项。默认情况下，除非 MTU 不匹配，PnPGW 不对用户 TCP 报文的 MSS option（默认 1460，即 1500-IP 头长度-TCP 头长度）进行强制改变。一个常见的需要对 TCP MSS 进行强制修改的应用是 ADSL/PPPoE 拨号，因为此时 MTU 为 1492，此时系统必须能动自动调整 TCP MSS < 1452 以避免用户的 TCP 应用异常，PnPGW 在进行 PPPoE 拨号后会自动调小 TCP MSS。在极少数情况下，运营商的出口路径或者不同运营商之间的路径可能存在 MTU 不匹配现象，若发现此问题导致某些 TCP 应用异常，则需要强制使用较小的 TCP MSS，直到测试异常 TCP 应用恢复正常。比如 set force_tcp_mss 1432。

为了系统资源安全，PnPGW Enterprise 于 2006 年 6 月后发布的版本后增加防范 P2P 下载和基于 MAC 地址安全策略的防 ARP 广播攻击或假 IP 攻击的功能。命令行：

set deny_bt on|off 打开或关闭防 P2P 下载功能。

show deny_bt 显示匹配丢弃的 P2P 下载报文数，分 BT 和 Emule 统计。

所谓 mac 安全策略，是指每个 mac 地址，在规定时间间隔内，当达到系统指定的最大 arp 表项创建或冲突更新计数，或 session 创建计数，则列为 mac 黑名单，来自黑名单 mac 的 ARP 表项创建/更新或者新建 session 请求将被系统丢弃。mac 黑名单可在 4 小时或者指定超时时间内由系统自动清除，或者由管理员手动删除。命令行：

set black_mac_chk on|off 打开或关闭 MAC 安全策略功能。

set black_mac_timeout <minute> 配置黑名单 mac 的超时删除时间，默认 240 分钟，也就是 4 小时。

set black_mac_threshold <interval> <arp> <session> 配置 MAC 安全策略参数：

第一个参数<interval>为单位探测间隔，默认 60 秒。

第二个参数<arp>为最大 arp 表项创建或更新指标，默认 5。

第三个参数<session>为最大 session 创建次数指标，默认 5。

set black_mac_threshold 60 5 5 意即某 MAC 地址在 60 秒内，发出了 5 次导致系统新建或者冲突刷新 ARP 表项的 ARP 请求，或者发出了 5 个不同源 IP 的 IP 报文导致系统新建立 5 个 session，那么就列进系统 MAC 黑名单。注意当命令行输入 set black_mac_threshold 配置参数合法时，系统将自动启用 MAC 安全策略，即自动配置 set black_mac on。

show black_mac 列出当前黑名单 mac， 每条黑名单包括 mac 地址，被列为黑名单时记录的 arp 和 session 计数，被列为黑名单状态的时长(秒)。

no black_mac [mac] 删除黑名单 MAC，当不带 mac 参数，则清空当前所有黑名单 MAC。

为了尽最大可能保证中病毒或者木马的用户上网正常，对于已列入黑名单 MAC，仍然允许如下例外：

1. 用户经过正常的 DHCP 流程获取了 IP 地址，允许匹配的 MAC/IP 创建 session 和 ARP 表项

2. 用户已经 UP 在线，允许匹配的 MAC/IP 创建 ARP 表项

3.16 no

用法：

no user/servicename/snmp name

no port enet[0/1/2/3] vlan_id <id> <num>

no port enet[0/1/2/3] second_ip

no dhcp address ip num

no dhcp relay ip net

no dhcp agent

no dhcp enet[1/2/3] input

no session address ip num

no session ip

no blck_mac [mac]

说明：

no usr/sevicename/snmp 删除本地帐号、服务，SNMP 团体名。

no port enet[1/2/3] vlan_id <id> <num> 删除端口上的 VLAN 配置。

no port enet[0/1/2/3] second_ip 删除端口上的第二个 IP 地址配置。

no dhcpaddress/relay/agent 删除 DHCP 地址池、中继配置。

no dhcp enet[1/2/3] input 禁止端口开启 DHCP 功能。

no session address 删除接入地址段等配置。

no session ip 强制用户下线。

no black_mac [mac]删除系统黑名单MAC地址，见3.15 MAC安全策略描述。

例如:

no user admin

删除 admin 本地帐号。

no servicename serv1

删除名字为 serv1 的服务。

no dhcp address 10.1.1.2 253

删除 10.1.1.2 的 dhcp 地址段。

no session ip 10.1.1.7

强制 IP 地址为 10.1.1.7 的用户下线。

3.17 ping

用法：ping <ip>

说明：使用 icmp echo 检测目标地址的连通性。

例如:

> ping 202.96.196.5

检测目标地址为 202.96.196.5 的连通性

3.18 pnp

用法：

pnp enable|disable

pnp dns direct|redirect

```
pnp smtp redirect <ip> [all]
pnp http_proxy redirect <ip> <port>
pnp pass enable|disable
pnp pass enable nonportal
pnp upnp enable|disable|list|clear
pnp no_arp_pub enable|disable
pnp ignore|no_ignore <ip> <mask>
pnp bridge bind <ip> <mac> [gw]
pnp bridge unbind <ip>
pnp delete <ip>
pnp netbios enable|disable
```

说明：配置 IP PNP 功能，使得满足绝大多数用户自配 IP 的情况都可以上网。

pnp enable|disable 启用或者关闭 PNP 功能

pnp dns direct|redirect 设置用户自行指定 dns 时如何处理，redirect 指定用户的 DNS 请求强制转向到 primary DNS，direct 则使用用户自己的 DNS。为保证 PNP 效果，一般使用 pnp dns redirect。

pnp netbios enable|disable 为 PnPGW 3.3 新增命令，启用或者关闭 netbios 名字解析欺骗功能。Netbios Name Service 是 windows 办公网络的一项常用服务，为同 LAN 中 windows 主机解析 NetBIOS 主机名，比如文件、打印、代理服务器等。对于用户认证时在 IE 里输入不可解析的域名或者 NetBIOS 主机名，或者将 HTTP 代理设置为原办公环境中使用的 NetBIOS 主机名的特殊情况，启用 pnp netbios enable 就可以保证用户正常接入到 ineternet。

pnp smtp redirect <ip> 强制转向所有用户的私网目的地址的 SMTP 请求到指定的 SMTP 发信服务器的 IP 地址。当 ip 参数为 0.0.0.0 时，禁止 SMTP 强制转向。由于用户发邮件是个很频繁的行为，所以若使用 SMTP 强制转向时，要求外部配置的 SMTP 服务器运行可靠，DNS 配置正确，而且能接受所有不认证或者认证的 SMTP 请求。当启用 all 选项，则强制转向用户的所有 SMTP 请求。注意 all 选项是个过时配置，当要强制转向所有 SMTP 请求，应使用 nat 配置，源地址子网指定为 0.0.0.0/0 即可，比如当 SMTP 服务器 IP 为 218.1.4.36，那么相应的 nat 配置为 nat add rdr enet1 0.0.0.0/0 srcport 25 218.1.4.36/32 dstport 25。

pnp http_proxy redirect <ip> <port> 强制转向用户的 http proxy 请求到指定的 http proxy server。PnPGW 内置实现了 http proxy server，绑定 8080 端口，只接收来自 E1 端口的请求，所以一般配置成 pnp http_proxy redirect <enet1 的 IP 地址> 8080 即可。也可指定转向到外部的 http server，ip 应设置为外部代理服务器的 ip 地址，port 可以设为 80，8000，8080，3218 等，应与外部代理服务器设置 port 号一致。

pnp pass enable|disable 启用或者关闭 PnPgW 作为一个不认证/计费的 IP PNP 网关。当 pnp pass enable 时，所有用户被推送的首页都是一个简单的连接页面，不需要输入用户名和密码。当需要认证计费时，则配置 pnp pass diable。

pnp pass enable nonportal 是pnp pass的特殊情况，不要求用户在上网时一定先使用WEB浏览，也不强制用户一定经过Portal过程才能接入到PnPGW，用户感觉就象使用普通路由器在上网。从 2.5 的 20040427 build版本开始，PnPGW开始支持nonportal模式的pnp pass。对于nonportal模式的pnp pass在的实际使用注意问题，见FAQ章节 4.8的描述。

pnp no_arp_pub enable|disble 启用或者关闭与 PnPGW E1 口同子网段的 ARP 欺骗。默认情况是 disable 的，这样保证若用户自配的 IP 地址落在 E1 子网段内，但是网关没有指向 E1 口的 IP 地址，也能够使用户正常上网。通常在酒店宽带运营中，客房和办公位于不同的子网段，但是有些酒店由于条件所限，客房和办公网是混在一起的，且办公网与 E1 同子网段，此时造成办公网用户发出的非上网业务相关的 ARP 请求（ARP 请求的目的地址不是 E1 口的 IP 地址）被欺骗造成这些业务不正常，比如打印、文件共享等，这种情况下建议配置 pnp no_arp_pub enable，使得办公网的正常业务不被 PnPGW 的 ARP 欺骗

行为所干扰。

pnp upnp enable|disalbe|clear 启用或关闭PNP功能、列出或清除当前UPNP维护的NAT转向（RDR）规则集。从 2.5 的 20040427 build版本开始，PnPGW开始支持UPNP协议，以支持类似MSN音频/视频这样需要UPNP协议支持才能正常穿越NAT的应用在私网环境下能够正常使用。由于安全问题（注意是潜在的DoS攻击风险），以及MSN新版本逐渐开始不依赖UPNP进行音频/视频流NAT穿越，从Enterprise 060223 版本开始，PnPGW默认设置为pnp upnp disable。注意当PnPGW的E0 口没有公网地址的情况下，一定要保证配置成pnp upnp disable。对于pnp upnp命令使用以及涉及UPNP实际使用中需要注意的问题，见FAQ章节 4.9的描述。

pnp ignore|no_ignore <ip> <mask> 使得 PnPGW 在 E1 口不对来自为<ip>/<mask>子网段的 ARP 请求进行欺骗，参数中 ip 为子网段的网络地址，mask 为子网掩码。自 pnpgw 2.5 的 2005 0118 build 版本起增加了对该命令的支持，该命令可完全替代 pnp no_arp_pub enable 的作用，而且更灵活。pnp no_arp_pub enable 只能使 PnPGW 不干扰与 E1 口同子网段的 ARP 欺骗，而 pnp ignore 命令可以设置 PnPGW 不干扰任意子网段的 ARP 欺骗，包括与 E1 口同子网段的，或者不同子网段的。pnp no_ignore <ip> <mask>可取消相应子网段的 pnp ignore 配置。

以下是一个常用的 pnp 配置，E1 端口的 IP 地址为 172.31.13.1：

```
# pnp enable
# pnp dns redirect
# pnp http_proxy redirect 172.31.13.1 8080
# pnp pass enable
# pnp no_arp_pub disable
```

以下是一个跟 pnp ignore 命令相关的特殊配置。E1 端口的 IP 地址为 172.31.13.1，掩码 255.255.255.0，酒店办公网的主机也处于同 E1 相同网段，占用了 172.31.13.224/255.255.255.224，另外该酒店开通了 IP TV，IP TV 的终端通过另一不经过 PnPGW 的出口动态获得 IP 地址段为 10.0.4.0/255.255.254.0 的地址，为防止 PnPGW 对办公网的文件共享/打印，以及对 IP TV 终端进行 ARP 欺骗造成干扰影响正常业务，增加如下 pnp ignore 配置：

```
# pnp ignore 172.31.14.224 255.255.255.224
# pnp ignore 10.0.4.0 255.255.254.0
```

PnPGW 还提供如下跟增强 HTTP 代理支持相关的 pnp 配置命令：

```
pnp http_proxy port <port ...>
pnp http_proxy detect high|nomal
```

pnp http_proxy port <port ...> 可一次配置最多 6 个检测端口，当端口参数与默认端口(8080，80，8081，8000，3128)冲突，可自动忽略，比如：pnp http_proxy port 9000 8888 9001，使得 pnpgw 在判断 http 端口时除了检测用户的默认端口外，还检测 TCP 9000/8888/9001 端口。

pnp http_proxy detect high|nomal，默认为 normal。normal 配置时，pnpgw 只对用户私网目的地址或者与用户同 B 的目的地址的 HTTP proxy 配置进行探测,当使用 high 配置时，对用户任何目的地址 proxy 配置都进行强制检测。注意 pnp http_proxy detect high 在用户上网时没开启使用浏览器访问 WEB 资源前，对于一些使用了 HTTP 或者代理的应用有副作用，比如 MSN 的第一次连接可能会失败,此配置一般只用在免认证无 portal 或者客房 VLAN 用户在选择策略周期内可使用无 portal 认证的场合。

20060223 之后发布的 Enterprise 版本增加 pnp bridge 命令支持，提供了“公网 IP 透传”功能，允许给位于 E1 下的主机和设备配置与 E0 口同子网段的 IP 地址（通常为公网 IP 地址），以满足特殊主机或者网管设备的公网地址透传需要。典型的应用是在 E1 下部署 VoIP 或者视频会议设备，或者在 E1 下部署酒店自用的 VPN Server 等。

pnp bridge bind <ip> <mac> [gw] 配置一个透传 IP 绑定，ip 和 mac 参数分别为所需要透传的 IP 地址和配置该 IP 地址主机的 MAC 地址，当 MAC 地址指定为 00:00:00:00:00:00 时，表示为动态透传 IP 绑定。gw 为可选参数，为该主机所配置的默认网关，一般不需要配置。注意若 ip 地址与 E0 同段，需要配合适当的 proxyarp 配置，类似 NAT 和 vpool 配置。

pnp bridge unbind <ip> 取消指定 IP 地址的透传绑定。

pnp delete <ip> 删除一个 ARP 欺骗记录，注意用户在线 session 若存在则删除失败。当需要绑定的透传 IP 已被其它配静态 IP 地址的用户占用时，可先使用 no session <ip>和 pnp delete <ip>进行删除操作，然后再使用 pnp bridge bind 命令进行透传绑定。

应用举例，比如 PnPGW 的 E0 为 202.83.4.2，上行出口为 202.83.4.1，掩码为 255.255.255.240，需要将 202.83.4.13 分配给 E1 下的一台视频会议设备，视频会议设备的 MAC 地址为 78:06:17:38:05:80，则视频会议设备的 IP/mask 配置为 202.83.4.13/255.255.255.250，网关指向 202.83.4.1，相应的，PnPGW 则做如下配置：

pnp bridge bind 202.83.4.13 78:06:17:38:05:80

proxyarp add 202.83.4.13 255.255.255.255

此时 show psgw 可以看到绑定透传的 IP/MAC 记录，Flag 为 1。相比较而言，动态绑定使用起来更为方便，动态绑定的 Flag 显示为 2。当动态绑定对应的 IP 被使用时，show psgw 可以看到绑定记录的 MAC 地址不为 00:00:00:00:00:00，而是用户的实际 MAC 地址，当用户 session 下线后，MAC 地址又恢复为 00:00:00:00:00:00，动态绑定记录的 IP 又处于可用状态。

当所透传 IP/MAC 的流量发生时，show session 可以看到用户名为 pnpbridge 的用户 session，注意被透传 IP 的用户 session 建立时，其带宽限制规则与 pass 的 session 一致。所以 session pass_in/out_rate 的配置应符合透传 IP 设备或主机的带宽需求。

3.19 port

用法：

port enet[0/1/2/3] ethernet <ip> <mask>

port enet[0/1/2/3] second_ip <ip> <mask>

port enet0 pppoe_c

port enet[0/1/2/3] vlan_id <id> <num>

port show

说明：配置端口的 IP 地址、VLAN。如果改变了 E0 口的端口模式，比如将 E0 口从静态 IP 地址改变 PPPoE 拨号，需要为 reboot 重新启动 PnPGW。另外，改变了接入端口（通常为 E1 口），或者启用第二个端口 IP 也需要重新启动 PnPGW。

例如:

port enet0 ethernet 192.168.1.10 255.255.255.0

把端口 E0 配置 ip 地址为 192.168.1.10，掩码为 255.255.255.0

port enet1 ethernet 218.1.43.1 255.255.255.192

port enet1 second_ip 172.31.13.1 255.255.255.0

把端口 E1 配置 ip 地址为 218.1.43.1/255.255.255.192，并配置第二个 IP 地址为 172.31.13.1/255.255.255.0。

port enet1 vlan_id 101 20

允许 E1 端口终结 802.1Q VLAN ID 从 101 开始到 120 共 20 个 VLAN ID。

port enet0 pppoe_c

设置 E0 端口启用 PPPoE 拨号。该命令需要配合 pppoe_c 命令指定帐号和密码，详见 pppoe_c 命令说明。

port show

显示当前所有端口配置。

3.20 pppoe_c

用法：

pppoe_c user <name> passwd <passwd>

pppoe_c start|stop

pppoe_c show

说明：配置和管理 E0 口的 PPPoE 拨号，使得 PnPGW 可以在上行链路为 ADSL 或者需要 PPPoE 拨号的 LAN 的情况下使用。

pppoe_c user .. passwd 配置 PPPoE 拨号的用户名和密码。

pppoe_c start|stop 使 PnPGW 开始 PPPoE 拨号或断开 PPPoE 连接。

pppoe_c show 查看当前的拨号状态，在 PPPoE 拨号成功后，显示获得的 IP 地址/掩码信息。注意当 PPPoE 拨号成功后，系统的 ppp0 端口将会配置 PPP 协商获得的 IP 地址/掩码，而系统的默认路由将指向 PPP 连接远程对端接入设备的 IP 地址，这些改变可以通过 show link [ppp0]以及 show route 查看到。

E0 口使用 PPPoE 拨号时，通常配合 nat auto 配置实现自动的 NAT 转换，由于 PPPoE 拨号不能保证很长时间的在线，有时候会断开重拨，此时候出口公网地址改变，需要自动更新所有和出口 IP 相关的 NAT 规则。详细见 NAT 的命令说明。

以下是个将 PnPGW 的 E0 口配置为 ADSL 拨号模式的例子，假设 ADSL 帐号为 adsl200411，密码为 testpass，则配置如下：

port enet0 pppoe_c

pppoe_c user adsl200411 passwd testpass

nat auto

3.21 proxyarp

用法：

proxyarp add/del <ip> <mask>

proxyarp show

说明：代理一段 IP 地址的 ARP 应答。当 NAT 的目的转换 IP Pool 是与本地子网同段时(与上行以太端口 E0 同一子网段)，proxyarp 可配合 nat 命令，使得上端路由不添加该段的路由也能正确将目的 IP 为这段 IP 地址的报文正确发送到 PNPGW 上行端口。

注意当 mask 不为 255.255.255.255 时，<ip>参数必须是和<mask>参数能相匹配的子网地址。

例如：E0 端口的 IP 地址为 202.14.87.212，掩码为 255.255.255.240，属于子网段 202.104.87.208/255.255.255.240，内网 E1 地址为 182.168.1.1/255.255.255.0，指定 202.104.87.212-215 四个 IP 地址用于 NAT 规则的转换目的 IP 池，此时的设置应该为：

nat add map enet0 192.168.1.0/24 202.104.87.212/30 portmap

nat add map enet0 192.168.1.0/24 202.104.87.212/30

proxyarp add 202.104.87.212 255.255.255.252

除了配合 NAT 外，proxyarp 还用于用户端被物理或者 VLAN 隔离、而相互间需要通信的情况。比如用户处于 IP 地址为 192.168.1.0/24 的子网段，而用户间被 vlan 一一隔离，192.168.1.16/255.255.255.240 网段的用户间需要互相通信，那么就可以配置：

proxyarp add 192.168.0.16 255.255.255.240

3.22 radius

用法：

radius [b]auth/[b]acct/dupacct ip <ip> key <key>

radius [b]auth/[b]acct/dupacct retry <num>

radius [b]auth/[b]acct/dupacct timeout <seconds>

radius [b]auth/[b]acct/dupacct port <port>

radius [b]auth/[b]acct/dupacct enable/disable

radius show

说明：配置 RADIUS 认证服务器和计费服务器，auth 和 acct 配置首选认证和计费服务器 IP，bauth 和 bacct 是配置备份

的认证和计费服务器 IP，dupacct 是复制帐单的 Radius 计费服务器，即 Radius 计费包同时发往 acct 及 dupacct 指定的 Radius 计费服务器，注意 dupacct 指向的服务器 IP 一定与 acct 指定的 Radius 服务器不同。timeout 和 retry 配置与 Radius 服务器通信的超时和最大重发请求次数。

例如:

```
# radius auth enable
# radius auth ip 202.96.196.2 key secret_key
# radius acct enable
# radius acct ip 202.96.196.2 key secret_key
```

以上启用 radius 认证和计费，指定 radius 服务器 IP 为 202.96.196.2，通信密钥为 secret_key。

```
# radius auth timeout 5
```

认证请求如 5 秒没收到应答， 将重发请求

```
# radius auth retry 3
```

认证请求最大重发次数为 3。

3.23 radtst

用法: radtst <username> <password> <service> [vlan_id]

说明：与当前配置的 radius 服务器进行通信测试，模拟对某用户帐号的认证行为。

例如：

```
# radtst 1112 1112 internet 112
```

说明：使用当前的 radius 对帐号 1112 密码 1112 帐号选用的服务为 internet VLANID 为 112 进行模拟认证。

系统模拟将会返回认证结果以及相关授权属性，示例如下：

```
send radius auth [1112][1112][internet][112], waiting for reply...
Amtium-Max-Up-Rate: 512(上行带宽限制)
Amtium-Max-Down-Rate: 512(下行带宽限制)
Amtium-Redirect-Url: http://www.sohu.com(用户强制URL向)
radius auth success(表明帐号可用，认证成功)
```

当与 Radius 通信失败时，将显示 timeout，可能的原因有几点：

1. PnPGW 与 Radius Server 网络上没有连通
2. PnPGW 的 Radius Server 配置的通信密钥配置错误
3. Radius Server 没有将 PnPGW 加入到 NAS 列表，或者加入了但是通信密钥配置错误

3.24 reboot

用法：reboot

说明：重启设备。在改变某些敏感配置(例如端口、地址池)后或根据需要重新启动 PnPGW。若 reboot 命令被执行时若有 Radius 认证用户在线，那么 PnPGW 将会强制这些用户下线，并送出计费包，延时一段时间后在重新启动设备，以最大程度保证用户帐单不丢失。可以看到执行了 reboot 命令后，串口上会显示“ acct-stop sent for 整数 up session(s) ”的信息。

3.25 route

用法：

```
route add/del <net> <mask> <gateway>
route show
```

说明：添加/删除静态 IP 路由，显示系统路由表信息。

例如:

```
# route add 0.0.0.0 0.0.0.0 202.96.196.5
```

增加缺省路由为 202.96.196.5

route show

显示系统的路由表信息。

3.26 servicename

用法：servicename <name>

作用：定义宽带服务的名称。在用户认证时，该服务名称将作为一个私有 Radius 属性提交给 Radius Server。不同于安腾面向电信/企业的 D-BrAS 接入服务器产品，PnPGW 不是面向多服务的接入服务器，因此配一个缺省的 internet 服务名即可。

例如:

servicename internet

定义服务的名称为 internet

3.27 session

用法：

session address <begin_ip> <num> [pass] [rate <uprate> <downrate>]

session echo_timeout <second>

session echo_interval <second>

session acct_alive <minute>

session acct_interval <minute>

session pass_in_rate <kbits/s>

session pass_out_rate <kbits/s>

session idle_chk enable/disable

session idle_timeout <minute>

session idle_data <kbits>

session max_nat_num <num>

session web_num <num>

session admin enable/disable

session spam_threshold <concurrent> <interval> <count>

说明：

session address 命令配置某段 IP 为认证 IP 地址段，从这段 IP 发来的包受到 PnPGW 监视，用户认证过后可以进行正常的包转发，否则只能访问有限的 PnGW 资源，比如 PnPGW 的 WEB 服务、ping PnPGW 的接入端口 IP、进行 DNS 解析，并且上行带宽受限制。session address 的命令的参数中，<begin_ip>是该认证地址段的起始 IP 地址，<num>是起始 IP 地址开始的连续 IP 地址数量。pass 是可选参数，如果指定了 pass 参数，则表示此段地址的主机可以无需认证直接进行包转发，相当与专线用户，注意 pass 的 session 只有在对应 IP 的 arp 表项超时被删除后，才可被系统自动删除，因此当 pass 的用户 MAC 地址改变时，可能需要将原先存在的用户 session 手工 no session <ip> 删除。此外，session 命令还支持[rate <uprate> <downrate>]子句，能对 session 段 IP 地址指定限制带宽，这在 PnPGW 单独部署无外部 Radius 进行授权，而又需要对不同用户群限制不同带宽时比较方便。对于 PnPGW 来说，最常用的一个配置是配置相同的处于 E1 子网段的 dhcp address 和 session address，例如 E1 地址为 172.31.13.1/255.255.255.0，那么配置

dhcp address 172.31.13.2 253

session address 172.31.13.2 253

使得处于 E1 端口的所有用户，必须通过认证后才能上网。

session echo_interval 设置 PnPGW 多长时间主动用单播 ARP 探测用户（单播 ARP 探测只用于用户选择了可能使用 VPN 的情况），缺省设置 90 秒。

session echo_timeout 命令设置用户与 PnPGW 间的 Keep-Alive 的超时时长，单位为秒。表示多长时间内，用户端与 PnPGW

间无有效 ARP Keep-Alive 应答，则视用户端断线，切断其连接并计费（多出的无效探测时长不会被计费），缺省设置 180 秒。PnPGW 的 ARP 探测行是每到 echo_interval 到就有三次间隔 10 秒的连续发送机会，只要其中一次成功，则停止发送，直到下一 echo_interval 超时到。因此 echo_timeout 比 echo_interval 大 20 秒以上就基本能保证准确探测用户下线（有两次以上探测机会）。对于有时长计费的场合，echo_interval 适当调小到满足用户拔线后短时间内就下线计费的需求即可。比如用户要求 1 分半内探测用户下线，按如下配置：

#session echo_interval 60

#session echo_timeout 90

注意 PnPGW 的新版本已经不再使用用户端主动的 WEB Keep-Alive。

session acct_interval <minute>设置 pass 的 IP 段主机间隔多少分钟发一次 Radius 计费包。当参数为 0 时表示不为 pass 的用户发计费包。酒店运营场合通常不需要为专线用户进行流量计费的场合，建议配置 session acct_interval 0。

session pass_in_rate 和 pass_out_rate 指定 pass 用户的带宽限制。为避免专线用户过度占用系统带宽，一般推荐为 pass 用户指定一个合适的带宽限制参数，比如指定 pass 用户带宽限制为上下行都为 1Mbps：

session pass_in_rate 1024

session pass_out_rate 1024

session idle_*配置全局的用户闲时下线检测参数。session_idle_chk enable/disable 启用或关闭用户闲时下线检测。session_idle_timeout 配置闲时下线的时长，session idle_data 配置闲时下线的流量下限。比如配置用户 15 分钟内流量小于 1kbits，则视为用户下线：

session idle_chk enable

session idle_timeout 15

session idl_data 1

注意对于酒店里的宽带应用，商务客人一般都希望长时间在线，因此可不启用 idle_chk enable，或者设置比较长的 idle_timeout，比如 30 分钟以上。若启用 idle_chk，为防止有在线窗口存在的情况下发生 idle-timeout 引起客人投诉，可以配合 webp online_win close 关闭小窗口。在必须使用在线小窗口的场合，为防止 idle-timeout 发生，可以修改相关页面脚本，使在线小窗口发出 WEB Keep-Alive，保证用户不发生 idle-timeout。见 FAQ 描述。

session max_nat_num 设置每用户的最大 NAT 会话数，以保护 PnPGW 的 NAT 会话资源不被过度占用。对于正常用户来说，120 到 150 左右的 NAT 会话是足够用的，对于中了蠕虫病毒的用户，用户的 NAT 会话数将会很快达到上限，导致无法上网。show session 命令可以查看每个认证用户的 NAT 会话数。

session web_num 设置每用户的最大并发与 PnPGW 的 TCP 80 连接数，PnPGW 的 TCP 80 为系统关键资源，必须防范用户无限制连接导致服务不正常。PnPGW 的 session web_num 建议设置在 20 到 25。

session admin enable/disable 允许或者禁止处于 session address 地址段的用户对 PnPGW 进行 WEB 管理或者 Telnet。默认的配置是 session admin disable。

session spam_threshold <concurrent> <interval> <count> 配置可在使用SMTP强制转向的情况下（见3.18的相关描述），防范中邮件蠕虫病毒的用户大量发送病毒邮件，或者防范不规范用户进行垃圾邮件群发。第一个参数<concurrent>为用户最大并发SMTP TCP连接指标，默认 5，第二个参数<interval>为最小探测时长间隔，默认 300 秒，第三个参数<count>为最小探测间隔内的最大SMTP累计连接次数，默认 20 次。session spam_threshold 5 300 20 的配置意即当用户SMTP并发连接达到 5 个，或者在 5 分钟内有过 20 次SMTP连接行为，那么就标记用户为垃圾邮件用户。

一旦用户发送邮件行为达到指定指标被设置垃圾邮件标记，被标记的用户无法再使用本地 smtp 转发，也不能直接访问

本地 smtp 服务器，只能使用自己原先的 smtp 服务器进行发信。用户一旦被设置垃圾邮件标记，那么用户被标记时刻的 SMTP 行为指标就会被记录下来不会改变直到用户下线重新认证，以方便管理员查看当前的垃圾邮件用户。show spam 命令可以查看当前的垃圾邮件用户以及 SMTP 行为指标。注意 session spam_threshold 功能只有当配置了 nat 来完成 SMTP 强制转向时才能生效，使用 pnp smtp redirect 配置时则无效。

show session_cfg 可以查看系统当前的 session 配置。

session acct_alive <minute>为 PnPGW Enterprise 里新增加的配置，该配置启用后，可为在线用户定时发送增量 Account-Alive 计费报文，每发送一次增量计费报文，用户的上线时间都会重新设置，流量/时长计费信息也都会被清 0，使用 show session 可以观察到。<minute>参数设置为 0 则禁用 acct_alive。

session acct_alive 配置主要是为了解决长时不下线用户的计费丢单（PMS Check-Out 无法强制用户下线）问题，以及用户连续几天在线导致一条 PMS 清单包含几天的费用引起的计费疑问和纠纷问题。注意非 Enterprise 版本 HBMS 的 RADIUS server 不支持 Accounting-Alive。当配合 HBMS Enterprise 版本使用时候，session acct_alive 配置启用后就可为在线用户每隔一段时间就发送一次 Accounting-Alive 报文（每次发送后流量和时长都清零，而 RFC 标准为累积不清零），可减少上述丢单或者计费纠纷问题。注意 2006 年 6 月后发布的 HBMS Enterprise 支持跨天点自动计费且不影响用户在线状态，可以彻底杜绝跨天清单现象。session acct_alive 配置比较适用于酒店房间有需要包天计费的固定 PC 的情况。

比如：
session acct_alive 15 则每 15 分钟发送一次计费增量报文。

注意当 session idle_chk enable 或者用户选择计费策略功能打开的情况下，用户每次 acct-alive 发送的计费时长并不一定等于 acct_alive 间隔，甚至为 0。因为有 idle_chk 或者用户有效期存在的情况下，计费时长总以用户有无发生有效流量为准，计费时长自上次 acct-alive 结束后开始重计，当本次 acct-alive 间隔到发送增量计费信息时，时长只算到最后一个有效流量报文发生的时间，若本次 alive 间隔根本没发生流量，那么时长就肯定为 0。

实际应用中建议，纯包天/包月类计费环境可以不打开 session idle_chk，因为 HBMS Enterprise 可以实现对纯包天/包月类用户一上网就计费，而不是下线才计费。若需要使用 idle_chk，那么建议：acct_alive 间隔 > idle_chk 时长。比如：

```
session idle_chk enable
sesison idle_timeout 15
session acct_alive 20
```

当使用了时长计费包天策略，建议：包天封顶时长 > acct_alive 间隔。比如 1 元/分钟，包天封顶 60 元，则 acct_alive 间隔 < 60 分钟即可，比如 30 分钟。

3.28 show

用法：show <var>
说明：显示系统的各种状态信息
例如在配置状态下执行 show 命令的结果：

```
# show ?
Usage:
show config              -- show all configuration
show port                -- show port configuration
```

```
show pppoe_c              -- show pppoe client configuration
show session     [ip]     -- show  sessions
show route                -- show route table
show radius               -- show radius configuration
show arp                  -- show arp table
show proxyarp             -- show proxyarp table
show netstat              -- show network connections
show ipstat               -- show ip statistics
show tcpstat              -- show tcp statistics
show udpstat              -- show udp statistics
show icmpstat             -- show icmp statistics
show user                 -- show user
show servicename          -- show servicename configuration
show hostname             -- show hostname configuration
show nameserver           -- show nameserver configuration
show version              -- show system verion
show auth                 -- show authentication type
show set                  -- show system set
show snmp                 -- show snmp community
show dhcp                 -- show dhcp configuration
show pnp                  -- show plug and play configuration
show psgw                 -- show connect pseudo gateway
show multi                -- show multicast service state
show spam                 -- show spam users
show deny_bt              -- show deny bt statistics
show black_mac            -- show black mac list
show session_cfg          -- show session configuration
show webp                 -- show web portal configuration
show system               -- show system tasks CPU utility
show bwstat               -- show online and bandwidth statistics history
show ?                    -- show help
```

show version 和 show config 是查看系统版本、配置常用到的命令，在进行系统配置、排错若遇到疑难问题，通常需要将这两个命令的结果提交给相关技术支持人员。

以下 show 命令在观察系统状态时常用到：

show ip/tcp/udp/icmpstat 显示当前 IP 转发统计、TCP/UDP/ICMP 统计；

show netstat 显示当前 tcp/udp 连接和服务状态；

show arp 显示当前 ARP 表；

show route 显示当前路由表；show psgw 显示当前伪网关应答记录；

show session 显示当前在线用户；

show link 显示端口报文（包括组播报文）的收发统计；

show memory 显示内存分配使用情况；

show mbuf 显示系统网络层使用缓存的统计情况；

show task 显示系统当前任务状态；

show system 显示系统当前各任务 CPU 利用率情况；

show bwstat 显示过去过去 72 小时内的在线、平均/峰值上下行带宽采样数据，每 15 分钟一组采样数据。

show spam显示当前垃圾邮件用户。见3.27节session spam_threshold配置描述。

show deny_bt显示被丢弃的P2P下载报文统计。见3.15节set deny bt on|off描述。

show black_mac显示当前系统MAC黑名单。见3.15节set black_mac描述。

3.29 show session

用法：show session [ip]

show session_pass

说明：show sesison [ip]显示所有或者指定 IP 地址的在线用户状态，包括时长、流量、包等。show session_pass 显示所有专线用户状态。

例如：

show session

显示所有在线用户结果用户

Name	IpAddress	MAC	VLAN	Status	Time	NAT	CHK
	172.31.13.34	001422c78303	0	INIT	40	1	WEB
2004	172.31.13.6	0000f0928087	0	UP	10208	23	ARP
1102	172.31.13.22	001422fcfa51	0	UP	12877	8	ARP
1000	172.31.13.4	0014bf1ba391	0	UP	17127	12	ARP

UP/ALL session number: 3/4

show session 命令为每用户显示一行信息，第一列为用户帐号，第二列为 IP 地址，第三和第四列为 MAC 和 VLAN，第五列为用户状态（INIT 未认证、AUTH 正在认证、UP 认证成功），第六列为保持当前状态的时间，单位为秒；第七列为用户当前的 NAT 会话数；第八列是 PnPGW 探测用户是否在线的类别，WEB 为用户 IE 小窗口主动 ECHO 探测，ARP 为 PnPGW 主动单播 ARP 探测，IDLE 表示使用闲时探测。

show session 172.31.13.170

显示 IP 地址为 172.31.13.170 的用户的在线时长、状态和流量信息，以下是 200606 发布的 PnPGW 的 show session <ip> 显示信息：

name	1000		
online	420	status	UP
mac	001422c77bab	vlan_id	0
chk	arp_alive	ctrl	0x00000000
uprate	512	usage	0
downrate	1024	usage	0
inPkts	1480	outPkts	1432
inBytes	208472	outBytes	1225484
http_pcb	0	nat_num	2
icmp_cnt	0	arp_cnt	0
spam_flg	0	smtp_cnt	0 0
upnp_pcb	0	upnp_maps	0
rdr_addr	203.156.209.187	proxy_st	0
rec_addr	172.31.13.1	rec_port	80
rec_smtp	0.0.0.0	rec_dns	0.0.0.0

online 显示已在线时长（秒），当用户为卡用户或者选择策略用户，还将显示用户本次的最大允许在线时长（秒）及入流量空闲时长（秒），参数名分别为 timeout 和 idle_in。ctrl 为用户扩展控制参数，需要和 2006 年 06 月后发布的 HBMS Enterprise 版本配合，ctrl 参数为 32 位无符号整数，每一位都可以定义自己控制功能，目前只用到其中 5 位：

当（ctll & 0x01）非 0，禁止 vpool 分配

当（ctll & 0x02）非 0，禁止 SMTP 强制转向

当（ctll & 0x04）非 0，禁止 P2P 下载

当（ctll & 0x08）非 0，禁止 ARP keep-alive，强制 idle timeout

当（ctrl & 0x80）非 0，那么该用户 timeout 最大在线时长到不断线自动计费，主要应用于包天时间点到自动计费防止出现跨天清单

用户使用的系统资源以及系统安全的相关参数： uprate/downrate 为带宽分配参数，usage 表示上一次采样带宽，in*/out*为上下行流量统计参数。http_pcb 是用户当前与 PnPGW 的 HTTP 连接数，nat_num 是用户当前的 NAT session 数，upnp_pcb 是用户当前的 UPNP TCP 连接数，upnp_maps 是当前用户 UPNP 规则数，icmp_cnt 和 arp_cnt 为系统 arp/icmp 流控功能记录的上一个探测间隔内用户累计的 icmp 和 arp 计数，spam_flg 和 spam_cnt 显示用户是否被标记为垃圾邮件用户，以及上一个探测间隔内的 smtp 并发和累积连接计数。

其它状态参数： rdr_addr 表示用户被分配到的 vpool 地址，rec_addr 记录了用户被强制转向到 Portal 界面前，想访问的 IP 地址，proxy_st 为用户当前的 PROXY 配置判断状态，若 proxy_st 为 1，则表示 PnPGW 判断用户使用了 HTTP proxy，此时 rec_addr 就是用户所配置 HTTP Proxy 的 IP 地址，而 rec_port 则为代理端口。rec_stmp 和 rec_dns 记录用户被 pnp 转向的原 smtp 和 dns 配置。

show session_pass 显示当前在线直通或者专线用户，与认证用户不同，忽略用户名和 keep-alive 类型，例如：

```
# show session_pass
IpAddress        MAC             VLAN   Time    NAT   In/OutPkts
172.31.13.250    0030f155e5b8    0      203399  0     2407/2242
Total pass session: 1
```

3.30 snmp

用法：

```
snmp com name  r|w|rw
snmp trap ip
snmp trap_version <version>
```

说明：设置 SNMP 网管平台相关配置信息。snmp com 设置 SNMP 团体名，r|w|rw 表示网管信息权限，r 表示读，w 表示写。snmp trap 设置 trap 信息的目的地址，当目的地址为 0.0.0.0 时，表示不启用 snmp trap。snmp trap_version 设置 snmp trap 的版本类型。

例如：

```
# snmp com amtium rw
# snmp trap 192.168.1.1
# snmp trap_version 1
```

以上设置 SNMP 团体名字为 amtium，trap 目的 IP 为 192.168.1.1，trap 版本为 1。

对于酒店工程，若 RADIUS 也是安腾的产品，要求 snmp 的团体名和 radius 的 key 一致。

3.31 telnet

用法：telnet <ip> [port]

说明：telnet 到其它设备或者服务器。port 是可选参数，默认即 telnet 服务使用的 TCP 23 端口。

3.32 time

用法：time [YYYYMMDDHHMM]

说明：显示和修改系统时间。在初次配置设备时，通常要设置好系统时间。

例如:

time

显示系统时间

time 200012031200

设置系统时间为 2000 年 12 月 03 日 12 时 00 分。

3.33 upgrade

用法：upgrade <tftp_server> <file_name>

说明：通过 tftp server 升级系统 IOS，重启后可运行新的 IOS

例如:

upgrade 202.96.196.3 pnpgw25.bin

到 ip 地址为 202.96.196.3 的 tftp server，下载文件名为 pnpgw25.bin 的文件作为系统新版本 IOS。

3.34 user

用法：user name <name> passwd <passwd>

作用：增加本地用户。若配置了 local auth enable，即允许本地认证，则本地用户也可以通过 PnPGW 完成接入上网。

例如:

user name admin passwd pass

增加一个名字为 admin 密码为 pass 的本地用户。

3.35 vlanuser

用法:

vlanuser <username> vlan <vlan_id>

vlanuser del <vlan_id>

vlanuser auth <radius/local>

vlanuser show

说明：vlan 认证设置。当使用 radius 方式的 VLAN 认证时，PnPGW 将会从 vlan_id/帐号对应表中尝试查询 vlan_id 对应的帐号名称，查询成功则将帐号做为 Radius access request 的 Username 属性，而将 vlan_id 作为安腾的私有 vlan_id 属性提交给 Radius Server，使 Radius Server 可以配合完成 VLAN 认证。当 vlan_id 对应帐号关系查找失败时候，PnPGW 则直接将 vlan_id 的数字串填写进 access request 的 Username 属性，和私有 vlan_id 属性一起提交给 Radius Server。

vlanuser <username> vlan <vlan_id>设置 VLAN 号映射到帐号的对应关系，对应关系中，vlan_id 是主键，当执行 vlanuser .. vlan 命令，而指定的 vlan_id 已存时，将覆盖该 vlan_id 旧的对应关系。

vlanuser del 删除指定 vlan_id 的帐号对应关系。

vlanuser auth 指定 vlan 认证方式，是本地或 radius 认证，一般本地 VLAN 认证只是用来调试，正式运营时总是选择 radius 认证。

vlanuser show 列出当前所有的 vlan_id 和帐号的对应关系。

例如：

vlanuser 1112 vlan 112

添加一个 VLANID 为 112 与帐号为 1112 的映射。

vlanuser del 112

删除一个与 VLANID 为 112 对应的帐号映射。

vlanuser auth radius

vlan 认证采用 radius 方式认证。

为支持高端酒店 VLAN 认证环境的选择计费策略、一次或无 Portal 控制、公共区域漫游/无线区域登记漫游等运营特性，PnPGW 的 Enterprise 版本增加了以下 vlanuser 配置命令：

vlanuser policy enable|disable|renew|show|debug

vlanuser policy timeout <seconds>

vlanuser policy port <port>

vlanuser policy pub_vlan <vlan_id> <num> [wlan]

vlanuser policy del pub_vlan <vlan_id> <num>

vlanuser passwd_push enable|disable

说明：HBMS Enterprise 上实现了一个策略服务器，可提供包括可选计费策略、VLAN Portal 策略和 MAC 地址认证策略信息。PnPGW Enterprise 可定时连接策略服务器取得上述策略数据。当允许 VLAN 认证用户 Portal 选择策略或者 Portal 控制，PnPGW Enterprise 就访问策略服务取得可选计费策略列表供用户登录时选择，取得 VLAN 策略以区分哪些 VLAN 用户需要 VLAN Portal 认证、哪些 VLAN 用户需要选择策略的 Portal 认证、哪些 VLAN 用户无 Portal 认证。当允许 VLAN 认证用户漫游到 LAN 公共区域，PnPGW Enterprise 就访问策略服务取得 MAC 地址列表允许这些 MAC 地址在公共区域使用 MAC 地址认证，免除 Portal 密码认证的麻烦。WLAN 公共区域的处理则有所不同，用户电脑的 WLAN 网卡 MAC 通常和 LAN 网卡 MAC 不同，因此用户在房间的 VLAN 认证登记的 MAC 无法漫游到 WLAN 公共区域，因此需要在用户房间 VLAN 认证成功时推送密码给用户，此后用户第一次在 WLAN 区域上网时需要用此密码进行 Portal 认证上网，成功后 HBMS Enterprise 自动登记 WLAN MAC 到数据库中，之后用户再到 WLAN 区域上网就使用 MAC 认证而不再需要 Portal 认证。

vlanuser policy enable|disable|renew|show|debug

enable 则启用 vlan 认证用户的策略服务，disable 禁用，renew 强制刷新计费策略列表，show 查看配置

debug 查看当前策略内容，包括可选计费策略列表，用户 vlan 状态和 mac 状态

vlanuser policy timeout <seconds>配置策略刷新时间间隔，默认为 30 秒，PnPGW 每到策略刷新时间间隔到，都会请求 HBMS 端的 VLAN Portal 策略服务，取回当前的 VLAN 和 MAC 列表策略数据。计费策略列表刷新数据间隔则比较长，为固定 30 分钟，因此若在运营过程中 HBMS Enterprise 端更改了可选计费策略列表，需要使用 vlanuser policy renew 来尽快刷新计费策略列表。

vlanuser policy port <port>，配置 HMBS 策略服务 TCP 服务端口，默认为 1404。

当需要启用公共区域 MAC 漫游认证时候，使用以下命令进行配置：

vlanuser policy pub_vlan <vlan_id> <num> [wlan]配置公共 VLAN 区域，加 wlan 选项表示为 WLAN 区域

vlanuser policy del pub_vlan <vlan_id> <num>删除公共 VLAN 区域

vlanuser passwd_push enable|disable

enable 启用 vlan 认证用户推送公共区域密码服务，disable 禁用

vlanuser passwd_url [url]

默认的Server端URL为http://radius_ip:8080/user/notepass.php，当另需定制其它URL时，比如radius的WEB服务端口改变，或者使用其它页面时，可用此命令行另行配置推送密码页面

3.36 vmap

用法：

vmap bind <mac> <vlan_id>

vmap unbind <mac>

vmap query/del <mac>

vmap list [vlan_id]

vpool show

说明：在有 VLAN 的环境，PnPGW 会维护 vlan-mac 映射关系表，以保证发送给指定 MAC 地址的报文通过查询 vlan-mac 表项后能封装正确的 802.1Q VLAN 头信息。vlan-mac 映射表项为一般为被动建立，当某 MAC 地址发送报文来自某 VLAN，PnPGW 就动态建立 vlan/mac 映射表项，为提高效率避免频繁的表项建立和删除，当累积到 32k 表项时，PnPGW 才自动删除超时 24 小时的表项。某些情况要求 vlan-mac 关系在开机就静态建立。比如位于 PnPGW 下的某些需要从外部可访问的网管设备，若完全使用动态建立的 vlan-mac 表项，当 PnPGW 重新开机后，网管设备还没有发出任何报文，此时设备对应的 vlan-mac 表项没建立，那么从外部访问此网管设备就会失败。

vmap bind <mac> <vlan_id> 配置静态 vlan-mac 绑定，系统启动就生效，适用于需要从外部访问的网管设备、透传 IP 设备等，系统重启后映射关系不变，注意当 mac 移从到其它 vlan 时，绑定关系中的 vlan 信息自动跟随改变。

vmap unbind <mac> 取消 vlan-mac 静态绑定。

vmap query/del <mac> 查询或删除指定 mac 地址的对应 vlan 信息。

vmap list [vlan_id] 查询某 vlan_id 或者所有的 vlan-mac 映射关系，当不指定 vlan_id 参数，表示查询所有 vlan 内的映射关系。为防止表项过多查看不方便，使用 vmap list 时系统会自动删除超时 24 小时的表项。

vmap show 显示当前的 vmap 绑定配置。

3.37 vpool

用法：

vpool add <ip> <num>

vpool del <ip> <num>

vpool ignore|no_ignore <ip> <mask>

vpool show

说明：单一出口网关设备通常要使用 NAPT，NAPT 对只使用了 TCP/UDP 封装类型的应用支持得比较好，当 NAPT 时，IP 报头的地址信息和 TCP/UDP 报头的端口信息以及校验值等内容将被改变。而某些 VPN 类型不使用 TCP/UDP 类封装（比如 PPTP 的 GRE 和 IPSec 的 ESP），或者对 IP 之上的整个报文信息进行了完整性校验使得 NATPT 对 TCP/UDP 报头内容的改变非法，因此在 NAT 环境中，只使用 IP 转换和不使用 TCP/UDP 端口转换能保证最大程度地不影响 VPN 使用，而只使用 IP 转换就要求提供更多的出口公网 IP，使得多个用户能够同时使用 VPN。vpool 命令的作用就是配置和管理 VPN 用户专用的公网地址池。

vpool add/del 添加或者删除 VPN 地址池。

vpool ignore|no_ignore 添加或者删除忽略 vpool 地址分配的用户子网地址段，典型应用在 E1 口配置 second_ip 的情况，不需要为分配了公网地址的用户再进行 vpool 地址分配。典型配置如下：

port enet1 ethernet 222.66.89.193 255.255.255.224

port enet1 second_ip 172.31.13.1 255.255.255.0

session address 222.66.89.194 29

session address 172.31.13.2 200

vpool ignore 222.66.89.192 255.255.255.224

vpool show 查看当前的地址池分配情况。

同 NAT 配置类似，当 vpool 地址池与 E0 口 IP 地址同子网段时，需要配置相应的 proxyarp，如 E0 地址为 218.14.1.2，掩码为 255.255.254.0，218.1.14.1.1 为对端路由，同子网段的其它地址 218.14.1.3~14 分配作为 vpool 地址池，那么配置如下：

vpool add 218.14.1.3 12

proxyarp add 218.14.1.3 255.255.255.255

```
# proxyarp add 218.14.1.4 255.255.255.254
# proxyarp add 218.14.1.6 255.255.255.254
# proxyarp add 218.14.1.8 255.255.255.252
# proxyarp add 218.14.1.12 255.255.255.254
# proxyarp add 218.14.1.14 255.255.255.255
```

3.38 web

用法：

```
web put|get <tftp_server> <filename>
web upgrade <tftp_server>
web ls
web pr <filename>
web rm <filename>
web purge
```

说明：配置 web 页面文件。注意 PnPGW 不支持长文件名，只支持 8.3 格式的本地文件名，即 8 个字符以内的文件名，3 个字符以内的扩展名。

web put/get <tftp_server> <filename> tftp 更新或者保存 web 页面；

web upgrade <tftp_server> tftp 升级整个页面包；页面包通常发布为 rar 文件，管理员将文件接压到 TFTP Server 的文件目录下，在 PnPGW 上执行 web upgrade 命令后，PnPGW 则自动逐个 TFTP 获取每个页面文件；用 web get 或者 web upgrade 更新 web 页面文件后，需要使用 webp recache 使 web server 重新从 flash 中读取所有页面文件到缓存，或者 reboot 重新启动 PnPGW，见 webp recache 说明。注意 20060223 以后的 Enterprise 版本支持使用 web get <tftp_server> file.cfg 来获得特殊定制的 web 升级页面文件列表，当获取了 file.cfg 后，web upgrade <tftp_server>就会按照 file.cfg 里的文件名进行定制升级。file.cfg 文件内容格式为每文件名间用空格，TAB 或换行间隔，文件名必须为 DOS 文件的 8.3 格式，filc.cfg 文件最大为 4095 字节。

web pr <filename> 把 web 页面文件内容（如果是 dos 格式）打印在终端窗口；

web rm <filename> 删除 PNPGW 设备里的 web 页面文件；

web purge 删除当前使用的所有 web 页面文件，使用此命令要特别谨慎，注意事先做好必要的备份。另外，本命令忽略对 file.cfg 文件的删除；

web ls 显示 PNPGW 设备里的 web 所有页面文件。

要非常非常谨慎使用本功能，本功能为运营商定制网页而设，建议使用前先与安腾公司技术部门联系，否则可能会造成服务器崩溃。

例如：

```
# web get 192.168.1.100 cauth.asp
```

从 IP 为 192.168.1.100 的 tftp server 上下载文件名为 cauth.asp 的 web 文件。

```
# web upgrade 192.168.1.100
```

从 IP 为 192.168.1.100 的 tftp server 上下载整个页面文件包。

注意：可以使用 webp recache 命令把新上传的页面生效，不用重起设备就可以起效。

对于特殊定制的页面集合，文件名差异比较大，逐个对照升级比较麻烦，可事先定制好 file.cfg，然后按如下步骤进行：

```
# web purge
# web get 192.168.1.100 file.cfg
# web upgrade 192.168.1.100
```

重新启动或者 webp recache 即可。

3.39 webadm

用法：

webadm put|get <tftp_server> <filename>

webadm upgrade <tftp_server>

webadm ls

webadm pr <filename>

webadm rm <filename>

webadm online

webadm kick <user>

webadm lang auto|en

说明：配置 WEB 管理页面文件。注意 PnPGW 不支持长文件名，只支持 8.3 格式的本地文件名，即 8 个字符以内的文件名，3 个字符以内的扩展名。

webadm put/get <tftp_server> <filename> tftp 更新或者保存 WEB 管理页面；

webadm upgrade <tftp_server> tftp 升级整个 WEB 管理页面包；管理页面包通常发布为 rar 文件，管理员将文件接压到 TFTP Server 的文件目录下，在 PnPGW 上执行 webadm upgrade 命令后，PnPGW 则自动逐个 TFTP 获取每个管理页面文件。用 webadm get 或者 webadm upgrade 更新 web 管理页面文件后，需要使用 webp recache 使 web server 重新从 flash 中读取所有管理页面文件到缓存，或者 reboot 重新启动 PnPGW，见 webp recache 说明；

webadm pr <filename> 把 WEB 管理页面文件内容（如果是 dos 格式）打印在终端窗口；

webadm rm <filename> 删除 PNPGW 设备里的 WEB 管理页面文件；

webadm ls 显示 PNPGW 设备里的所有 WEB 管理页面文件；

webadm online 显示当前活动的 WEB 管理会话，每行五列，依次为用户 ID、帐号、会话标识符、源 IP、最近活动时间；

webadm kick <user> 按用户 ID 踢 WEB 管理员下线；

webadm lang auto|en 设置 WEB 管理界面的语言。该命令一般为调试用，配置结果不被保存，系统启动后总是为 auto，PnPGW 总是根据用户浏览器的语言类型自动会用户推松简体中文或者英文界面。执行 webadm lang en 可使 PnPGW 总是推送英文界面的 WEB 管理页面。

3.40 webp

用法：

webp url <address>

webp redirect_url enable|disable

webp service_url [URL]

webp online_win open|close

webp pass/nopass <ip>

说明：设置 WEB Portal 功能。

webp url 设置用户认证后强制转向的 URL 地址。

webp redirect_url enable|disable 设置启用或禁用用户认证后被强制转向 URL。

webp online_win open|close 设置用户认证后是否推送在线连接页面窗口。由于 PnPGW 通过 ARP Keep-Alive 可以实现用户拔线后短时间内就探测用户下线进行计费，因此可以关闭在线连接窗口。某些场合比如商务中心等固定电脑需要在线小窗口以方便用户能主动下线，可以在 HBMS Enterprise 里设置启用强制在线窗口的控制属性，参见 HBMS Enterprise 管理员手册。

webp service_url设置用户在线连接窗口的自服务URL。对于计费场合，service_url通常设置为计费系统所提供的自服务URL。安腾酒店计费系统的URL默认就是http://radius的IP地址:8080/。

webp pass/nopass <ip>设置或取消用户不认证即可访问的 IP 地址资源。

例如一个计费场合的 webp 配置：

```
# webp url http://www.amtium.com
# webp service_url http://192.168.1.100:8080/user/
# webp online_win open
# webp redirect_url enable
# webp pass 202.99.13.7
```

3.41 webp recache

用法： webp recache

说明：把 web 面文件重新读入内存。为提高效率，web server 只访问内存页面而不访问 flash 页面，所以对页面进行更改和升级以后，应使用 webp recache 把新版本的页面重新读如缓存使新页面生效。

3.42 webp vlan

用法:

webp vlan_page enable/disable

webp vlan <vlan_id> <num> pass [portal_file]

webp vlan <vlan_id> <num> <portal_file>

webp del vlan <vlan_id> <num>

说明：配置 VLAN 认证或者 VLAN Portal

webp vlan_page enable/disable 启用或关闭 VLAN 认证。

webp vlan <vlan_id> <num> pass [portal_file]，指定 VLAN 认证段，portal_file 为可选参数。默认的 VLAN 人证 portal 为 cvpass.asp 和 vpass.asp（英文）。若需要指定某 VLAN 段使用其它的 VLAN 认证页面，则需要制作好并上传相应的 VLAN 认证 Portal 页面文件，然后在 webp vlan .. pass 命令行中指定该 Portal 文件。注意 webp vlan .. pass 所指定的地址段必须先被包含在接入端口终结 VLAN 段内，即 port ..vlan 配置中。

webp vlan <vlan_id> <num> <portal_file>，指定 VLAN Portal。用户默认的 Portal 页面是 cauth.asp 和 auth.asp（英文）。若想指定某段 VLAN 使用其它的认证 Portal，则需要制作好并上传相应的认证 Portal 页面文件，然后在 webp vlan 命令行中指定该 Portal 文件。同样 webp vlan 所所指定的地址段必须先被包含在接入端口终结 VLAN 段内。

webp del vlan <vlan_id> <num> 删除 VLAN 认证或者 VLAN Portal 段。

通过以上命令可以实现 VLAN 认证，并可以使不同 vlan 区域弹出指定的认证页面，包括 vlan 认证或者用户/密码认证页面。例如指定 101-110 为正常用户密码认证，111-120 为另一修改过的用户密码认证页面 cauth_1.asp，指定 121-130 为 vlan 认证页面，而指定 131-140 为另一修改过的 vlan 认证页面，则配置为：

# port enet1 vlan_id 101 40	E1 口上终结 802.1Q VLAN 从 101 到 140
# webp vlan_page enable	启用 VLAN 认证或 VLAN Portal
# webp vlan 101 10	VLANID 为 101 到 110 的用户使用默认的用户名/密码认证 Portal 页面
# webp vlan 111 10 cauth_1.asp	VLANID 为 111 到 120 的用户的认证 Portal 为定制的用户/密码认证 Portal 页面 cauth_1.asp
# webp vlan 121 10 pass	允许 VLANID 为 121 到 130 的用户使用 VLAN 认证
# webp vlan 131 10 pass vpass_1.asp	允许 VLANID 为 131 到 140 的用户使用 VLAN 认证，VLAN 认证的 Portal 页面为定制的页面文件 vpass_1.asp
# vlanuser 1201 vlan 121	配置 VLANID 121~130 对应房间号 1201 到 1210，131~140 对应房间号 1301 到 1310
# vlanuser 1202 vlan 122	
# vlanuser 1203 vlan 123	

…

vlanuser 1301 vlan 131

vlanuser 1302 vlan 132

…

上面的各段 webp vlan 配置都可以使用 webp del vlan 删除，指定 vlan 段即可，比如：

webp del vlan 121 10

webp del vlan 111 10

3.43 write

用法：write

作用：将当前配置保存到 flash 中。

四、 常见问题以及排错手段

4.1 DHCP 用户可获得地址但是打不开认证或连接页面

可能的现象及原因如下：

1. DNS 相关故障，DNS 不可靠将导致用户域名解析失败，从而导致发不出 HTTP 请求导致 Portal 过程失败。对于 IE 来说，会提示“找不到服务器或发生 DNS 错误”的信息。排错人员测试可以在用户端用 nslookup 工具测试，也可以在 PnPGW 上用 ping <域名>的命令来判断 DNS 解析是否流畅。另外，如果用户输入的 URL 本身就是个不可解析的域名，也将导致 Portal 过程失败；
2. Proxy 设置问题。PnPGW 支持常用的 HTTP Proxy 端口包括 80，8080，8000，3128 和 8081，除了这五个端口之外，不支持其它端口设置的 HTTP proxy；另外，当用户配置了 SOCKS Proxy 时，也将导致 Portal 过程失败，因为 PnPGW 目前不支持 SOCKS proxy。
3. IE 的自动配置代理问题。新版本的 PnPGW 均可支持自动代理发现，升级 IOS 和页面即可。

4.2 PNP 用户打不开认证或连接页面问题

PNP 用户的 Portal 故障问题同样也可参考 4.1 节。PNP 用户能否成功接入的一个重要前提就是 ARP 欺骗成功。若 ARP 欺骗成功，则用户主机的 ARP 表（Windows 可用 arp –a 查看）显示默认网关 IP 对应的 MAC 地址为 PnPGW 的 E1 口 MAC 地址，同时 PnPGW 的 show psgw 可以看到伪网关应答记录，记录用户的 IP 地址、MAC 地址和请求解析的网关地址。PNP 不成功的可能原因如下：

1. 用户没有配置 DNS。没有配置 DNS 将导致用户根本发不出 DNS 请求，所有 DNS 解析就必然失败，DNS 解析失败则必然导致浏览器无法发出 HTTP 请求，进而导致 Portal 过程失败；
2. 用户没有配置网关，除非此时用户配了同子网段的 HTTP Proxy，否则是无法 PNP 成功的。原因是没有配网关时，用户主机的 IP 层就根本无法发出目的地址为非本主机子网段的 IP 报文；
3. 极端的配置冲突。当用户与 PnPGW 的任意一个端口的 IP 地址冲突、与 PnPGW 的任一静态路由网关冲突（一般只有默认路由）时，将导致 PNP 失败。

4.3 VLAN 以及 VLAN 认证相关问题

VLAN 或 VLAN 认证的常见问题如下：

1. 当 E1 口下配了多个 VLAN 时，用户机器自有 VLAN 覆盖的接入区域移动到没有 VLAN 覆盖的接入区域时，无法 Portal 或上网。这是因为当端口配了 VLAN 后，若用户处于 VLAN 区域，则 PnPGW 就将根据用户上行报文记录用户 MAC-VLAN 对应关系，当用户移动到另一个 VLAN 后，该对应关系将被更新，而当移动到非 VLAN 区域后，MAC-VLAN 对应关系并不会被删除，因此导致 PnPGW 回送给用户的报文失败。在组网时注意，若端口配置了 VLAN，那么要保证所有的

接入区域都要被 VLAN 覆盖；

2. VLAN 认证或者多 VLAN 配置中，PnPGW 串口出现类似“Dup Mac addr 12 位 MAC 地址 VLAN 号 VLAN 号”格式的告警信息。在 VLAN 认证或者多 VLAN 环境里，PnPGW 维护一张 MAC/VLAN 关系表，记录每个 MAC 地址所处的 VLAN，当某 MAC 地址从一个 VLAN 区域移动到了另一个 VLAN 区域后，会发生此告警信息。所以有两种可能，一种的测试人员将测试机从一个 VLAN 移动到另一个 VLAN，这是个正常现象；另一种就是跟 VLAN 相关的组网错误，当 PnPGW 的接入端口配置 VLAN 后，必须要满足 PnPGW 的接入端口作为整个二层网络唯一的 VLAN 终结点，另外就是保证接入区域内除非主机发生了 VLAN 区域移动，否则发送到 PnPGW 的报文只能有唯一的 VLAN ID 的 Tag 信息；
3. VLAN 认证或者多 VLAN 配置中，PnPGW 串口出现类似“Session Vlan VLAN 号 1 VLAN 号 2 error”格式的告警信息。这表明不同 VLAN 区域的用户发生了 IP 冲突。由于 VLAN 隔离了用户，所以用户终端不会出现 IP 冲突的提示。产生这个信息的原因是，处于 VLAN 号 2 的用户已经认证成功（Session UP 状态），而此时 VLAN 号 1 中的某个用户配置了与 VLAN 号 2 中已认证用户的相同 IP 地址。解决办法是查找出处于 VLAN 号 1 的这个用户，更改 IP 地址；
4. 使用了安腾的酒店认证计费系统的 VLAN 认证运营环境中，但是认证时提示“Invalid VLAN ID/VLAN 号错”。此时先要确认用户认证时，IE 窗口的标题显示的欢迎辞中的房间号与用户所处房间号是否一致，欢迎辞所显示的房间号是 PNPGW 根据 vlanuser 配置由 VLANID 查询出用户名显示出的，若一致，则再查询认证计费系统中的帐号/VLAN 对应关系是否和 PnPGW 中的 vlanuser 配置所设定的 VLANID/用户名对应关系一致；若不一致，说明 vlanuser 配置错误，或者 PNPGW 施工人员拿到的 VLANID/房间号关系表有错误；
5. 使用了安腾的酒店认证计费系统的 VLAN 认证运营环境中，用户已经 Check-In，但是认证时显示“Account not checked-in/帐号未启用”错误。此时仍需要确认用户认证时 IE 窗口的标题显示的欢迎辞中的房间号与用户所处房间号是否一致，若 vlanuser 配置错误指向了另一房间，而该房间没有 Check-In，则会发生上述错误。

4.4 常见串口告警信息

在调试过程中，有时串口上会打印出一些告警信息，常见的几类信息以及报警原因如下：

1. “源 16 进制 IP 地址 request another gw 目的 16 进制 IP 地址”信息。产生此信息的原因是，PNP 用户发出了多于一个目的 IP 地址的 ARP 解析请求，源 16 进制 IP 地址即是 PNP 用户的 IP 地址，目的 16 进制 IP 地址即是该用户正在请求解析的目的 IP 地址。PnPGW 会监视所有用户的 ARP 信息，通常自配 IP 的 PNP 用户的用户只在上网时发出解析默认网关 IP 的 ARP 请求，但有时 PNP 用户还会请求与自己 IP 同子网段的其它地址的 ARP 请求，最常见的就是用户除了配置同子网段的一个 IP 作为默认网关外，同时还配置了同子网段的另一个 IP 作为 HTTP Proxy。正常用户发生的 ARP 请求是很少的，因为 ARP 请求一旦成功用户主机就将结果记录 20 分钟以上这期间不会再对同一目的 IP 发 ARP 请求。当 request another gw 这个信息发生不频繁时，不会对设备和其它用户正常使用产生影响，但这个信息发生很频繁时，有可能是该用户中毒或者恶意攻击行为。比如有些蠕虫病毒会扫描本子网段的所有 IP 地址，发送 IP 地址时自然就会发送 ARP 请求信息，此时可能导致大量的 request another gw 信息，短时间内导致 PnPGW 消耗资源服务不正常。从 2.5 build 1115 版本开始，PnPGW 的 IOS 开始具有防范类似 ARP 攻击行为的能力，对于所有 PNP 或者 DHCP/固定 IP 的接入用户，都进行 ARP 流量控制。
2. “16 进制 IP 地址 arp 次数 times in 秒数 sec”。表示 E1 口下的 DHCP 或者其它同 E1 子网段固定 IP 用户，在几秒内发出了 10 次以上的 ARP 请求。同上一条描述，PnPGW 除了对 PNP 用户，还对 E1 口下的其它 DHCP 或者固定 IP 用户同样有 ARP 流控限制，每 2 秒才允许一次 ARP，产生此信息的最大可能就是用户中了蠕虫病毒或者正在进行恶意攻击。
3. “16 进制 IP 地址 exists in arp table， discard”信息。当 E1 下的 PNP 用户的 IP 地址与 E0 或者 E2 所处的子网段，而该 IP 地址对应的 ARP 信息又存在时候（表示 E0 或 E2 下有配置该 IP 的主机存在），则产生此告警。此时候用户 PNP 将失败，用户必须更改 IP 地址后，才能 PNP 成功。见 4.2 节的第三条描述。一个常见的过程能导致该现象发生，就是网管人员连接 E0/E2 做了网管或者上网动作后，不更改主机 IP 设置短时间内又把机器拿到 E1 口下尝试上网，而由于该主机的 ARP 信息仍在 PnPGW 的 E0/E2 口存在（持续 20 分钟才超时被删除），因此导致该现象发生，出现 exists in arp table 告警信息，上网失败。
4. “arp info overwritten for 16 进制 IP 地址 by MAC 地址”。ARP 表项的 MAC 地址信息改写报警。当有用户 IP 地

址冲突时候，PnPGW 收到来自不同的 MAC 地址的同一源 IP 地址 ARP 请求时，MAC 地址内容将被更改，从而产生此报警。

5. “arp info conflicted for 16 进制 IP 地址 by MAC 地址， discard”。由上条，用户 IP 冲突时，将导致 ARP 表的 MAC 信息被改写。为了保护不影响已经上网的用户已经重要主机的 IP 地址，当发生 IP 冲突时，PnPGW 不对已经认证的用户（session 状态为 UP 的用户）、正在使用的专线用户（配置 session address pass 且 ARP 表中有对应 ARP 表项存在）以及 ARP 绑定 MAC 的三类 IP 地址进行 MAC 更新，以保证这些用户的正常上网。当有用户试图抢夺上述受保护用户的 IP 地址时，串口上就会发生此信息。由此延伸的一个问题是，当专线用户更换主机或网卡时，若当时 ARP 表没超时，或者做了 ARP 绑定，那么会出现用户上网失败的现象，只要做 ARP 表删除或者重新绑定，即可排除故障。
6. “Dup Mac addr 12 位 MAC 地址 VLAN 号 VLAN 号”和“Session Vlan VLAN 号 1 VLAN 号 2 error”信息。见 4.3 节的第二条和第三条的详细描述。
7. “pnp forward_rt still not availabe”和“pnp forward_rt set to 端口名”信息。PnPGW 的默认路由存在时，才能保证 PNP 成功，当 PNP 服务启动时，若发现没有默认路由存在，则产生此报警，而当默认路由建立（添加默认路由命令或者 PPPoE 拨号成功），则产生后一条信息。

4.5 观察和获取系统信息

当有疑难问题发生，可以用 show 命令观察系统状态。

show link 显示每个端口的进出报文统计信息，特别是要观察 E1 口的统计信息，正常情况下，通常 E1 端口收到的组播（广播）报文占总共收到报文的比例不到 1/100，由于 PnPGW 要监视所有 ARP 请求信息，超过这个比例很多，则可能发生异常现象。间隔时间多获取几次 show link el1 可以大概估算当前 PnPGW 的 E1 口的进出包、进出组播/广播包增长速度。

show ipstat 可以观察当前的 IP 包转发情况。特别注意几个跟错误统计相关的字段，比如 bassum、redirectsent 和 nobuffers 字段值。间隔时间多获取几次 show ipstat，观察 forward 字段值增长可以大概估算当前 PnPGW 的包转发吞吐。

show mbuf 可以观察系统网络栈所用的缓存情况，若缓存被耗尽而长时间无法释放，则系统服务将会中断。

show task 可以观察系统当前任务的状态，特别要注意 tNetTask（网络层任务，主要负责包转发、NAT/ACL、ARP 解析等）和 tHttpd（Web Server）的状态。通常设备正常运行时，这两个任务都处于 PEND 或者 PEND+T 的阻塞状态。由于 WEB 认证要求 WEB Server 总是开放给用户的，PnPGW 对 WEB 资源以及 TCP 80 相关资源做了流控，但仍有可能出现 Web Server 遭受较高强度 DoS 攻击导致用户无法接入，此时可能可以观察到 tHttpd 任务处于 READY 状态，而 show netstat 里有大量未处理完的 TCP 80 连接。

当设备出现服务持续不正常而又无法使用正常手段排错时，可以将 PnPGW 串口上抓取的告警信息以及如下命令的结果（尽量在串口上执行）抓取发送给相关的技术支持和开发人员进行进一步排错处理：

```
show config
show session
show ipstat
show netstat
show link
show task
show mbuf
show psgw
```

4.6 如何由旧版本 D-BrAS 升级到 PnPGW

按如下过程升级即可：

1. 使用 D-BrAS 的 upgrade 命令升级 IOS 到 PnPGW 的版本，reboot；
2. 使用 web ls 列出当前 web 文件，web rm 逐个删除，若是 PnPGW 的 2004.12 以后 build 的版本，可以简单使用 web purge 命令删除所有的原 web 文件；
3. TFTP Server 指向 PnPGW 的 web 页面文件目录，web upgrade <TFTP Server 的 IP 地址>；
4. TFTP Server 指向 PnPGW 的 web 管理页面文件目录，webadm upgrade <TFTP Server 的 IP 地址>；

5. webp recache 或者 reboot；
6. 进行正常的 PnPGW 的 WEB 或者命令行配置。

4.7 用户配置浏览器代理的条件限制

当前发布的各个 PnPGW 版本，对 PNP 用户的代理配置有如下限制条件：

1. HTTP 代理端口为 80， 8080， 8000， 8081， 3128 之一，以及 pnp http_proxy port 多配置的其它端口；
2. 只支持 HTTP Proxy，不支持其它协议类型 Proxy，比如 SOCKS Proxy 和 FTP Proxy；
3. HTTP 代理的地址可以是 IP 地址，或者可解析的域名，而不能是不可解析的域名或者 NetBIOS 名字。PnPGW 3.3 版本支持 pnp netbios，IE 的代理可配置为不可解析的域名或者 NetBIOS 名字。

自 2.5 20040427 build 版本开始，可以通过 show session <ip>来观察用户配置代理的情况。

4.8 NONPORTAL 模式需要注意的问题

1. 注意 nonportal pnp 模式下的用户 session 配置， 对于非固定用户，最好不要把用户接入 IP 段配置成 session ... pass，session ... pass 在 PnPGW 里是面向固定或专线用户使用的，Keep-Alive 探测和 Idle-Timeout 机制对 pass 用户都无效，一旦 pass session 建立，只能等待 ARP 表项超时被动删除（大于 20 分钟），或者管理员主动手工 no session 强制删除；
2. 无 portal 接入模式下（包含不计费的 pnp pass enable，以及配合 HBMS Enterprise 实现用户选择计费策略，在选择计费策略周期内，不需要 portal 过程即可认证上网的情况），用户配置代理的默认发现条件：
   a. HTTP 代理端口为 80， 8080， 8000， 8081， 3128 之一，以及 pnp http_proxy port 多配置的其它端口，此点同有 Portal 模式
   b. HTTP 代理 IP 地址必须为 RFC 规定的私网地址， 或者跟用户配置的的静态 IP 地址在一个 B 地址段内

上述限制条件基本能满足绝大多数配置代理的情况， 即使有少数公司内部地址并不使用规范的私网地址， 其配置代理通常也不超过一个 B 的范围， 但是若该类不规范私网地址的用户在上网前将地址设置成 DHCP 而忘记去掉代理配置， 那么就可能产生 WEB 浏览故障。如果想达到和有 portal 配置模式下一样的代理支持效果，那么则需要提高代理探测级别，即配置 pnp http_proxy detect high 。

4.9 UPNP 的基本原理以及使用注意问题

UPNP 是一套由 Microsoft/Intel 等公司联合制订的协议标准，应用 TCP/IP 以及 HTTP/XML 使得网络设备之间增强互通和易用性，比如网络家电应用等。支持 UPNP 的网关设备可称之为 UPNP-IGD（Internet Gateway Device)。一些难以穿越 NAT 的应用程序可以向 UPNP-IGD 发出建立／释放 NAT 规则的请求，使其可顺利穿越 NAT，如 MSN 音频和视频应用。实现此机制的一个重要前提是客户应用程序本身也支持 UPNP。Microsoft 在 MSN 的 HELP 中说明，WinXP 内置实现了 UPNP，可在支持 UPNP 的网关下实现跨 NAT 的音频／视频通信，但是 Win2000 需要升级到支持 Direct 8.1 以上的 runtime 库才能使得 MSN 音频／视频支持 UPNP 和 NAT 穿越。

UPNP 用 1900/UDP 进行服务发现(SSDP 协议)，使用 2869/TCP 进行 NAT rdr 规则请求和释放的控制。支持 UPNP 的应用程序可使用 SSDP 广播发现支持 UPNP-IGD 的网关， 但是 MSN/Windows Messenger 则是直接向当前的默认网关直接发送单播 SSDP 请求以确认网关是否支持 UPNP。之后应用程序会在需要时，比如 MSN 需要建立音频连接时，向 UPNP-IGD 网关发出请求建立所需要的 NAT rdr 规则， 以使得应用程序的特殊 TCP/UDP 连接能够穿越 NAT 建立起来，当用户不再使用该 rdr 规则时， 会发出请求释放 rdr 规则。注意的有应用程序在 UPNP 行为上并不规范，在退出应用程序时，可能并不发出释放规则请求，导致 UPNP-IGD 累积过多的 rdr 规则。

UPNP 协议的行为特点决定了其本身是个不适合于在企业级网关或者大用户量环境下开放的协议,而更适合于 SOHO 环境，因为网关需要多开放 TCP/UDP 端口服务，另外 XML 语法解析相比使用固定字段长的协议解析更耗系统资源，因此必须有一定的手段来防范针对 UPNP 的 DoS 攻击。为防范系统抗 DoS 攻击，PnPGW 对资源分配做如下限制规则：

1. 总共 upnp rdr 规则数最大为 40，这样最多可支持 8 到 10 个用户同时使用 MSN 音频；
2. 每用户(UP 状态)最多可拥有 6 条 upnp rdr 规则。比如 MSN 语音一般建立 4 条规则，加视频 5 条足够；
3. 每用户(UP 状态)可并发发起 2 条 2869/TCP 连接。比如 MSN UPNP 的行为是顺序发起 TCP 连接，没有并发发出多个 UPNP TCP 请求。

另外，用户 logout 或者用户 session 闲置超时被删除了后，PnPGW 会自动删除属于该用户的所有的 upnp rdr 规则。这会带来一定副作用，比如当时用户 MSN 应用程序并没退出，而用户也没有拔除网线，那么当用户再认证上网以后，PnPGW 和用户双方间的 upnp rdr 就出现不同步现象，PnPGW 已经删除了该用户的规则，而用户的 MSN 会认为之前请求建立的规则还在，这样就可能导致 MSN 语音异常问题，此时用户重启机器，或者用户拔掉网线使 MSN 处于掉线状态后再插上网线，都可以解决问题。拔掉网线使 MSN 处于掉线状态可以使 MSN 认为网络不可用并把保存的所有 upnp 规则删除。所以实际使用中，应该提醒用户，logout 或者不上网了，一定要拔网线，以避免该副作用影响。

PNPGW 的出口 IP 必须配置公网地址时 pnp upnp enable 才有意义，否则应该使用 pnp upnp disable 关闭 upnp 功能。当对方也处于 NAT 网关后时， 那么要求对方的 NAT 网关也必须支持 UPNP-IGD 规范才能正常进行 MSN 音频视频通信。企业级的 Firewall 通常不支持 UPNP-IGD 规范， 或者因为安全原因不开放此功能，典型的如有些电信或 ISP 给用户分配私网地址，而电信或者 ISP 使用的 NAT 网关设备几乎是 100%不支持或者不开放 UPNP 功能的， 因此也就无法支持 MSN 音频应用。

4.10 如何防止在线小窗口存在的情况下发生 Idle-Timeout

由于 PnPGW 使用主动的 ARP keep-alive 来探测用户是否在线，因此默认情况下小窗口不再发出 WEB keep-alive 请求。为了防止在 idle_chk enable 情况下发生有小窗口的用户被 idle-timeout 引起投诉，需要对页面进行特殊修改，强制小窗口能发出 WEB keep-alive，WEB keep-alive 引发的流量即可避免用户被 idle timeout 下线。修改流程如下：

web get 导出 cconnect.asp 和 connect.asp，使用文本编辑器打开文件，找到以下两行：

```
var interval = <% websGetEchoTimer(); %>;
var deadtime = <% websGetDeadTimer(); %>;
```

如果要小窗口能 2 分钟(120 秒)发一次 WEB keep-alive 请求，稍大于 3 分钟(180 秒)无 WEB keep-alive 则小窗口自动退出，那么替换为：

```
var interval = 120000;
var deadtime = 185000;
```

web get/recache 更新两个文件即可。

注意，某些 VPN 可能会干扰 WEB keep-alive，其结果是用户拨了 VPN 一段时间内，小窗口因为 keep-alive 不成功会自动关闭，但是不会关闭用户的在线 session。

4.11 如何定制上网帮助邮件

把编写好的mail用foxmail发送出去（如果包含中英文以，发送时尽量使用UNICODE编码），然后到已发送邮件箱里，右键点击已发送邮件，原始信息->全部，将邮件内容拷贝下来，编辑信头，删除Date:头，使得接收邮件时总显示最新时间，from:头和to:头按情况改写，一般改成酒店或者运营商地址，比如from: hsia@shang-rila.com，to: vip@shang-rila.com，修改后保存为popnote.txt后，使用web get上传后，再启用E1 口的nat rdr 110 规则(见3.15描述)，即可实现未认证用户POP收取上网帮助邮件功能。

五、 附录

5.1 PnPGW 私有 Radius 属性列表

属性名称	属性值	属性类型	使用说明
Amtium-Max-Rate-Up	197	整型	为 Access-Accept 报文中的授权属性， 指定用户的最大上行带

			宽，单位为 kbps。PnPGW 控制带宽的最小粒度为 32kbps，因此赋值应为 32 的整数倍，0 表示不限制
Amtium-Max-Rate-Down	198	整型	为 Access-Accept 报文中的授权属性， 指定用户的最大下行带宽，单位为 kbps。PnPGW 控制带宽的最小粒度为 32kbps，因此赋值应为 32 的整数倍，0 表示不限制
Amtium-Vlan-ID	199	整型	为 Access-Request 报文中的认证请求属性，说明用户所属的 802.1Q VLAN ID，以配合实现 VLAN 绑定或者 VLAN 认证业务。有效的 VLAN ID 赋值为 1 到 4094。 当使用 VLAN 认证业务时候，PnPGW 首先尝试由 vlanuser 配置查找到用户所对应的帐号名称填写进 Username 属性，若没有查找到对应配置，则将用户 VLAN ID 转变为数字字符串填写进 VLAN ID，之后将 VLAN ID 的数字填写进 Amtium-Vlan-ID 属性，一起提交给 Radius Server 请求认证
Amtium-Servicename	200	字符串	为 Access-Request 报文中的认证请求属性，说明用户所请求的宽带服务类别，对于 PnPGW，通常只设定一种宽带服务，名称为 internet
Amtium-Redirect-URL	202	字符串	为 Access-Accept 报文中的授权属性， 指定用户被强制转向的首页 URL
Amtium-Portal-Key	203	字符串	为 Access-Request 报文中的认证请求属性，说明用户在 Portal 中所选择的计费策略表达关键字
Amtium-Portal-Cycle	204	整型	为 Access-Request 报文中的认证请求属性，说明用户在 Portal 中所选择的计费策略的周期数
Amtium-Misc-Cycle	205	整型	为 Access-Accept 报文中的授权属性， 指定用户的扩展控制属性，包括是否允许分配 VPN 地址池、P2P 下载、SMTP 强制转向和 ARP Keep-Alive 等