命令行使用说明书

2016 年 9 月

目　录

修订历史记录

修订日期	修订人员	更新说明
2015-12-08	Michael Li	撰写初步的命令行文档。
2015-12-21	Leo Shi	增加了文档的配置和使用说明。
2016-03-01	Leo Shi	更新了文档的格式。
2016-06-08	Yao Wu	新增对命令 ipsec、bw-bonus、arp announce 的配置说明。
2016-07-25	Yao Wu	新增对命令 traffic-control 的配置说明。
2016-08-25	Yao Wu	新增对命令 vrrp 的配置说明，调整部分命令位置顺序。

一、 综述

LinkBroad YunGW（以下简称 YunGW）是岭博科技（北京）有限公司的智能云网关产品，可广泛应用于商务人士较集中的中高端酒店以及商场、机场等 WIFI 热点覆盖区域，为需要宽带服务的商务人士提供宽带上网服务。

YunGW 可以单独部署于 Internet 出口为用户提供免费的上网服务，也可以与外部 RADIUS Server 配合实现用户认证和计费，提供收费的上网服务。

YunGW 可以与酒店的 PMS 系统进行对接，再与 LinkBroad BroadYun 酒店宽带云服务系统一起使用，BroadYun 酒店宽带云服务系统软件同时提供 RADIUS 标准 AAA(Authentication/Authorization/Accounting)服务，实现一个具备高可靠性、高可管理性的酒店宽带运营解决方案。

1. 设备型号和外观

LinkBroad YunGW 共有三个型号，分别是 2100，3100 和 5100，各个型号都带有 6 个 10/100/1000M 自适应 RJ45 以太网口。

2100 型号为 1U 标准高度，可最大接入 1500 并发用户；3100 型号为 1U 标准高度，可最大接入 5000 并发用户；5100 型号为 2U 标准高度，可最大接入 12000 并发用户。

YunGW 的网络端口、Console 口和状态灯都分布在设备前面板方便安装和观察状态，220V 交流电源插口和开关位于设备后面板。

YunGW 各个设备型号的前视图如下图 1-1 到 1-2 所示：

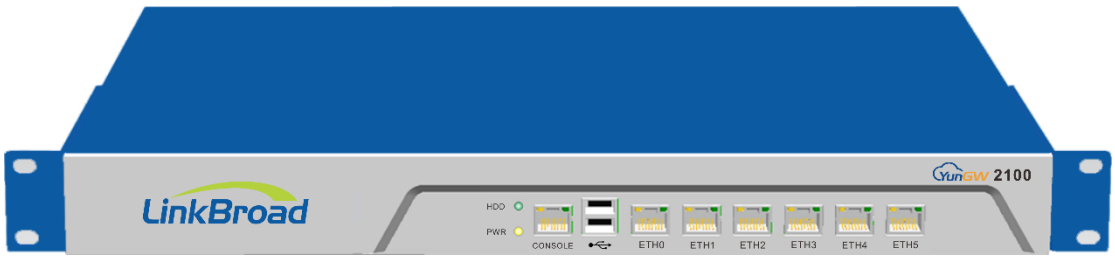


图 1-1 LinkBroad YunGW 2100

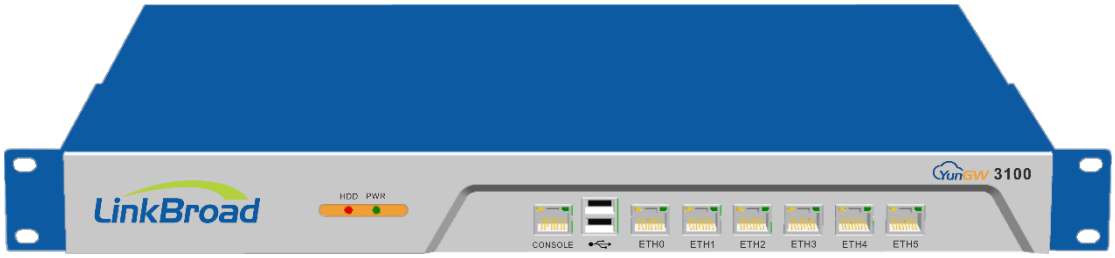


图 1-2 LinkBroad YunGW 3100

2. 硬件规范

YunGW 2100 的硬件规范如下表 2-1：

处理器和内存	物理端口
Intel Bay Trail J1900 CPU 4G RAM	6×Intel I211-AT RJ45 电口 1×RJ45 CONSOLE 口 1×RS232 串口 2×USB 2.0
电源	功率
220V 交流电源	60 瓦
外观尺寸	
440×300×44.5mm（1U）	
工作环境	
温度： 摄氏 0–40 度	相对湿度：5-95%

表 2-1

YunGW 3100 的硬件规范如下表 2-2：

处理器和内存	物理端口
INTEL I3 2120 双核 CPU 4G RAM	6×Intel 82583 RJ45 电口 1×RJ45 CONSOLE 口 1×RS232 串口 2×USB 2.0
电源	功率
220V 交流电源	200 瓦
外观尺寸	
440×300×44.5mm（1U）	
工作环境	
温度： 摄氏 0–40 度	相对湿度：5-95%

表 2-2

3. 设备安装及配置

3.1 设备安装

设备带有机柜上架配件，可以安装在标准机柜中。

YunGW 各个接口推荐接法如下：

ETH0 连接出口 ISP 的进线。

ETH1 连接核心交换机的上联口。ETH2-4 与 ETH1 有相同的功能。

ETH5 接入到交换机管理 VLAN 区域。

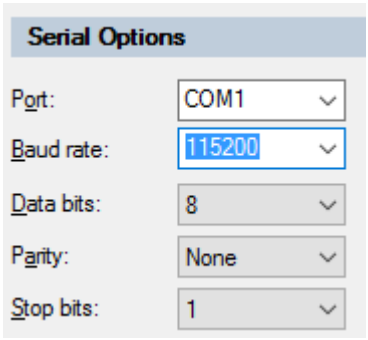
前面板的 CONSOLE 口连接配置电脑。

后面板的 RS232 串口连接酒店 PMS 接口

电源连接加电。

3.2 初步配置和命令行使用

使用串口连接 YunGW 配置时，波特率设置为 115200，数据位为 8。



连接成功后出现提示，默认 user 为 admin，Password 为 LinkBroad

命令行有多种模式，见表 3-1

命令行模式	提示符格式
基本用户模式	hostname%
超级用户模式	hostname #
终端配置模式	hostname-cfg #
端口配置模式	hostname-cfg-eth0 #

表 3-1

用户也可以用 SSH 远程登录后进行命令行配置，YunGW 的 Eth0 端口出厂默认配置为 192.168.98.199。

支持命令行?帮助，命令行 TAB 键补齐，语法错误提示等标准命令行操作特性。

YunGW 命令行特性见下表 3-2。

语法帮助	TAB 键，命令行单词补齐
	?键，命令行语法或单词帮助，如： # re? reboot - Reboot system remove - Remove object
	man <命令关键词>，查看命令语法全貌，比如， #man time NAME time - Set system time SYNOPSIS time sync time save
no 命令	YunGW 配置的删除，统一使用 no 命令行， 比如 no bypass all-users
remove 命令	所有删除 YunGW 在线信息的操作，都使用 remove 命令。 比如 remove online-user 10.10.20.5 remove login 6974

表 3-2

YunGW 命令行热键说明

常用热键	说明
CTRL-A	移动光标到行首
CTRL-B	向后移动光标 B=Backward
CTRL-C	中断占用终端的命令，比如 ping 或 show process cpu 等
CTRL-D	空行时相当于输入 exit 命令
CTRL-E	移动光标到行尾 E=End
CTRL-F	向前移动光标 F=Forward
CTRL-U	删除光标之前所有内容，不含光标所在字符 U=Undo
CTRL-K	删除光标之后所有内容，含光标所在字符 K=Kill
CTRL-W	删除光标之前一个单词 W=Word
CTRL-Y	在光标之前粘贴之前 CTRL-W 的内容
CTRL-R	搜索历史输入的匹配命令
CTRL-L	重新刷新当前输入行
上下箭头键	上下滚动查询历史输入命令
?键	提示命令行下一步匹配的关键字或参数语法

TAB 键	补齐关键字； 空行或光标前为空格状态，连续两次或以上的 TAB 键可获得一行或多行可用的关键字提示
回车键	输出滚动一行
空格键	输出滚动半页
其它任意可打印字符键	退出

3.3 端口配置指引

YunGW 端口的工作模式有两种，普通路由模式和接入控制模式(access control)。普通路由模式应用于出口 ISP 连接和网管端口，access control 模式应用于用户接入端口，目前支持 access control 模式的端口为 ETH1~ETH4 共 4 个端口，而且这 4 个端口同时都支持 PnP 功能。

YunGW 支持 802.1Q VLAN 终结，可以在接入端口上配置 1～4094 范围的 VLAN 号。ETH0 和 ETH5 端口只能配置为普通路由模式，ETH0 通常用于连接 ISP 出口设备，配置 ISP 指定的公网地址并配置默认路由后，使 YunGW 可以连接到 internet。ETH5 用于双 ISP 出口的第 2 个出口，或用于接入交换机管理 vlan，用于 snmp 管理或 PMS 连接。

ETH1 端口通常配置为 access-ctrl 模式，连接对客房和公共网络对用户进行认证和接入控制；如酒店有其他需求，也可以扩展使用 ETH2~ETH4 端口。

网关支持建立 GRE 的 vpn 连接。建议的规范配置中，tun0 端口用于连接 BroadYun。地址配置由中心统一给出。

网关同时支持作为 client 端建立 openvpn 的连接，固定端口 tun5 用于 openvpn 的 tunnel。

二、 命令详解

1. aaa-policy

aaa 认证的配置

说明	命令格式
指定的 vlan（或范围）不进行 MAC 地址认证	**mac-auth exclude-vlan** *<1-4094>* [*<1-4094>*]

设置允许账号漫游的 vlan 范围	**public-roaming vlan** *<1-4094>* [*<1-4094>*]
[关闭]开启 radius 认证	[**no**] **radius enable**
设置网关本地认证用户的 session 超时时间，单位分钟。	**radius local-session-timeout** *<30-1440>*
定义 radius nas-id	**radius nas-identifier** *name*
设置用户认证后的跳转链接	**radius redirect-url** *url*
设置 radius server 参数，默认端口为 1812 1813	**radius server ip-addr secret** *string* [**port** *<0~65535> <0~65535>*]
设置 radius 认证超时时间及重发次数 Timeout 时间范围为*<3-10>*，单位：秒 重发次数范围为<1-4>	**radius timeout** *<3-10>* **retries** *<1-4>*
开启[关闭]failover-bypass 功能：当网关探测到认证重发达到连续的 6 次以上时，自动切换为 failover-bypass 状态。该状态下，网关的所有用户免认证上网。当探测到认证恢复正常，网关切回正常认证状态。	[**no**] **radius failover-bypass enable**
查看 radius 认证配置	**show running-configuration aaa-policy**
查看 radius 状态信息	**show radius statistics**
查看 radius cache 的信息	**show radius cache**
查看 radius cache 的总数	**show radius cache statistics**
按 mac 查看对应的 radius cache 信息	**show radius cache** *mac-addr*
按 mac 删除对应的 radius cache 信息	**remove radius cache** *mac-addr*

mac-addr：设备的 MAC 地址，格式 xx:xx:xx:xx:xx:xx

name：nas-id 名称。

ip-addr：radius server IP 地址。

string：radius 认证的通信密钥

url：http://x.x.x 格式的网址

2. access-control 配置

2.1 arp-keep-alive、idle-timeout

说明	命令格式
开启 arp 在线探测	**arp-keep-alive enable**
网关每间隔时间进行 arp 探测，确认用户是否在线，当探测超时后，删除用户 session。 探测间隔时间范围为*<120-300>*单位：秒 探测超时时间范围为*<20-60>*单位：秒	**arp-keep-alive wake-up-interval** *<120-300>* **probe-timeout** *<20-60>*
Idle 探测模式时，单位时间内没有检测到用户流量，网关即删除用户 session。单位:秒。	**idle-timeout** *<300-1200>*

ip-addr：用户的 ip 地址。

2.2 bandwidth、connection-limit

说明	命令格式
设置接入用户的默认上下行带宽上限，前者为上行带宽，后者为下行带宽。 单位：kbps	**bandwidth default** *<100-1000000>* *<100-1000000>*
设置接入用户的默认连接数上限	**connection-limit default** *<10-10000>*

2.3 Bypass

说明	命令格式
[关闭]设置免认证 vlan 的范围 前者为起始 vlan 号，后者为结束 vlan 号	[**no**] **bypass vlan** *<1-4094>* *<1-4094>*
[关闭] 开启全局免认证	[**no**] **bypass all-users**

2.4 https-redirect

说明	命令格式
[关闭] 开启 https 页面重定向功能	**[no] https-redirect enable**

2.5 i-share

说明	命令格式
[关闭]开启 i-share 功能	**[no] i-share enable**
设置 i-share 互通带宽，单位 kbps 该带宽与用户上网带宽不同，是 i-share 用户之间的互访带宽值上限。	**i-share bandwidth** *<2000-20000>*
[取消]定义禁用甩屏功能的 vlan 段 前者是起始 vlan 号，后者是结束 vlan 号	**[no] i-share client-media-ctrl exclude-vlan** *<1-4094> <1-4094>*
[取消]定义甩屏设备 ip 段	**[no] i-share media-subnet** *net mask*
[关闭]开启 i-share soho-group 组 可以将不同的 vlan 划在同一个组里，从同组 vlan 上来的用户可以互相通讯。最多可以定义 8 个组。	**[no] i-share soho-group** *<1-8>* **vlan** *<1-4094> <1-4094>*

net：子网网络号。
mask：掩码。

2.6 listen-protocol、reject、trust

网关拒绝接入的地址范围及直通地址的设置

说明	命令格式
对于非 trust 用户，网关默认只识别两类报文来创建在线用户记录： 1. DNS 报文，UDP 目的端口 53 2. HTTP 类报文，允许 TCP 目的端口 80, 81, 3128, 443, 8080~9000 该命令允许发起 icmp 报文的用户创建在线记录（建立 session）	**listen-protocol icmp**
允许访问目的端口为指定 tcp 或 udp 的用户创建在线记录（建立 session）。	**listen-protocol {tcp | udp }** *<1-65535>*

设置拒绝接入网关的地址范围。	**reject** *addr-start1 addr-end1*
允许指定范围的 IP 地址直通上网，，同时可以定义他们的带宽（kbps）和连接数上限。	**trust** *addr-start2 addr-end2* [**bandwidth** *<100-1000000> <100-1000000>* **connection-limit** *<10-10000>*]

addr-start1：拒绝接入的用户 IP 段的起始 IP 地址。

addr-end1：拒绝接入的用户 IP 段的结尾 IP 地址。

addr-start2：直通用户 IP 段的起始 IP 地址。直通用户即网关设置的无需 portal，直接可以上网的 IP 用户。

addr-end2：直通用户 IP 段的结尾 IP 地址。

2.7 traverse

网关透传地址的设置

说明	命令格式
允许 IP 地址从一个接口透传到另一个接口。通常用于公网地址的透传。	**traverse** *ip-addr* **inside eth<0-3> outside eth<0-3>** [**mac-bind** *mac-addr*]

ip-addr：用于透传的 IP 地址。

mac-addr：与该透传 IP 地址绑定的 MAC 地址。

2.8 user-security

网关用户安全的策略设置

说明	命令格式
[关闭]开启泛洪保护 开启后每隔 5 秒检查用户的数据包，超过阀值的数据会被丢弃。同时会将用户加入 flood 名单中。	[no] **user-security flood-limit**
设置 dns 数据包的阀值，单位 pps（packets per second） 数值为正常通过认证的用户阀值，trust 用户是阀值数值*2，未通过认证的用户是数值减半。	**user-security flood-limit dns** *<20-300>*
设置 icmp 数据包的阀值，单位 pps	**user-security flood-limit icmp** *<5-50>*
设置 tcp 数据包的阀值，单位 pps	**user-security flood-limit tcp-syn** *<20-50>*

查看在线用户 flood-list 记录。注意，用户下线后会从名单中删除。	**show online-user flood-list**
[关闭]开启接入用户的 IP 访问隔离	**[no] user-security ip-isolate**
[允许] 阻止接入用户管理网关	**[no] user-security admin-prohibit**

2.9 weixin-wifi

说明	命令格式
[关闭]开启微信认证功能	**[no] weixin-wifi enable**
设置微信认证临时放行时间，单位：秒	**weixin-wifi bypass-timeout** *<30-300>*
[关闭]开启微信认证失败后放行的功能。开启后，用户临时放行时间用完后，将以 weixin@local 身份通过网关的本地认证。	**[no] weixin-wifi failover-bypass enable**

2.10 white-list

说明	命令格式
设置访问白名单。允许接入用户在没有通过认证时即可访问的 IP 地址、网址和相同域名后缀的网址	**white-list** { *ip-addr*[/<0~32>] | *domain* | **.domain* }
删除对应的访问白名单	**no white-list** { *ip-addr*[/<0~32>] | *domain* | **.domain* }
查看用户访问 white-list 中域名的解析情况。	**show white-list status**

ip-addr：白名单中的 IP 地址

domain：白名单中的域名

**.domain*：白名单中的带有相同域名后缀的网址，如：map.baidu.com news.baidu.com

3. dhcp 配置

3.1 dhcp 服务

说明	命令格式
指定 MAC 的终端获取 demand 地址池中	**dhcp demand** *ip-addr mac-addr*

的地址	
DHCP 池释放指定的 IP 地址	**dhcp release** *ip-addr*
撤销指定 IP 终端获取 demand 地址池中地址的操作	**dhcp revoke** *ip-addr*
[关闭]开启 DHCP 服务	[**no**] **dhcp service enable**
重启 DHCP 服务	**dhcp service restart**
查看 DHCP 地址释放时间	**show dhcp lease** [*ip-addr*]
查看 DHCP 运行状态	**show dhcp statistics**
查看 demand 的 dhcp 用户	**show dhcp demand**
查看 DHCP 配置	**show running-configuration dhcp**

3.2 dhcp subnet 配置

说明	命令格式
创建和进入 DHCP 子网段配置	**dhcp subnet** *network mask*
删除 DHCP 子网段	**no dhcp subnet** *network mask*
给指定的 MAC 分配指定的地址	**host-bind** *ip-addr1 mac-addr*
定义 DHCP 子网网关	**option default-gateway** *ip-addr2*
定义 DHCP 子网的 DNS	**option dns** *server1 server2*
定义 DHCP 子网地址释放时长，单位：分钟。	**option lease-time** *<3-1440>*
定义 DHCP 子网地址池范围 on-demand 表示地址池为按需分配预留，里面的地址平时不会分配出去	**pool** *addr-start addr-end* [**on-demand**]
给指定的 vlan 分配该网段 DHCP	**vlan-bind** *<1-4094>* [*<1-4094>*]

ip-addr1：DHCP 给指定的 MAC 分配的 IP 地址

ip-addr2：DHCP 子网的网关 IP

addr-start：DHCP 地址池的起始 IP 地址

addr-end：DHCP 地址池的结尾 IP 地址

network：子网网段

mask：子网掩码,格式样例：255.255.255.0

mac-addr：需要指定分 DHCP 的设备 MAC 地址

server1：DHCP 子网的主 DNS 地址

server2：DHCP 子网的备用 DNS 地址

4. interface 配置

4.1 interface eth 接口配置

说明	命令格式
进入 interface 配置模式	**interface** { **eth**<***0-5***> | **tun**<***0-3***> }
配置主[副]接口的地址	**ip address** *ip-addr mask* [**secondary**]
配置接口连接速率和双工模式	**speed** { **auto**|**10M**|**100M**|**1000M** } **duplex** { **auto**|**half**|**full** }
[关闭]开启端口的监听模式	[**no**] **access-control enable**
[关闭]启用接口的即插即用模式	[**no**] **i-nat enable**
查看接口配置	**show running-configuration interface**
查看接口状态	**show interface statistics** [**eth**<***0-5***> | **tun**<***0-3***>]

ip-addr：网关的接口 IP 地址

mask：掩码

secondary：副接口标识（可选）。

4.2 interface tun 接口配置

说明	命令格式
进入 tunnel 接口配置模式	**interface tun**<***0-3***>
建立 GRE 连接	**gre local-address** *lo-addr* **remote-address** *re-addr*
配置 tunnel 口的 IP 地址	**ip address** *ip-addr1* **peer-address** *ip-addr2*
配置 MTU 值，单位：byte	**mtu** <***1280-1476***>
[启用]关闭接口	[**no**] **shutdown**

lo-addr：建立 GRE 连接的本地端 IP 地址

re-addr：建立 GRE 连接的远端 IP 地址

ip-addr1：tunnel 接口的本地 IP 地址

ip-addr2：tunnel 接口的对端 IP 地址

num：MTU（最大传输单元）值，单位：字节，数值范围<1280-1476>

5. nat 配置

5.1 nat map 配置

说明	命令格式
配置 SNAT（源地址转换）转换规则 可以是 1 对 1、多对 1 或多对多	**nat** { **eth**<*0-5*> | **tun**<*0-3*> } **map** { *src-addr*[/<*0-32*>] } **->** *chg-addr1*[-*chg-addr2*]
删除对应的 nat 规则	**no nat** { **eth**<*0-5*> | **tun**<*0-3*> } **map** { *src-addr*[/<*0-32*>] } **->** *chg-addr1*[-*chg-addr2*]
清除所有 nat 规则	**nat flush-all-rules**
查看 nat 规则	**show running-configuration nat**
查看 nat 状态	**show nat status**

chg-addr1：SNAT 转换后的源 IP 地址，如果是多对多转换，该地址为转换地址池的起始 IP

chg-addr2：SNAT 源地址转换后的地址池结尾 IP 地址。

src-addr：SNAT 转换前的源 IP 地址或 IP 地址段

5.2 nat rdr 配置

说明	命令格式
根据目的地址（或范围）和目的端口进行 DNAT 地址转换	**nat** { **eth**<*0-5*> | **tun**<*0-3*> } **rdr** { **tcp** | **udp** } *dst-addr1*[/<*0-32*>] <*0-65535*> **->** *dst-addr2* <*0-65535*>
根据目的地址进行 1 对 1 的 DNAT 转换	**nat** { **eth**<*0-5*> | **tun**<*0-3*> } **rdr** *dst-addr3* **->** *dst-addr4*

dst-addr1：DNAT 的原始的目的 IP 地址

dst-addr2：DNAT 转换后的目的 IP 地址

dst-addr3：DNAT 1 对 1 转换前的原始的目的 IP 地址

dst-addr4：DNAT1 对 1 转换后的目的 IP 地址

6. openvpn 配置

说明	命令格式
上传 openvpn 的证书到 YunGW	**copy** *source_url* **openvpn-certificates**

证书文件的格式为 xxx.tgz,里面包含目录 openvpn，内含 3 个文件： server.crt openvpn 服务器证书文件 client.crt openvpn 服务器颁发给本站点的客户端证书文件 client.key openvpn 服务器颁发给本站点的客户端私钥文件	
删除 openvpn 证书(若 openvpn 已启用时操作无效)	**remove openvpn-certificates**
[关闭]启动 openvpn	**[no] openvpn enable**
配置 openvpn 的服务器地址及端口，目前只支持配置 udp 端口	**openvpn server** *ip-addr* **port** ***<0-65535>***
配置需要指向 openvpn 出口的网段或 IP 地址	**openvpn network** *net mask*
查看当前 openvpn 的状态	**show openvpn status**
可以查看 openvpn 的接口状态（tun5）	**show interface statistics**

ip-addr：服务器的 IP 地址。
net：网络号。
mask：掩码。
source_url：证书文件链接，格式： http://host/path，https://host/path，tftp://host/path， scp://user@host/path

7. ipsec 配置

说明	命令格式
[关闭]启用 ipsec	**[no] ipsec enable**
[删除所有的 ipsec 策略] 进入到 ipsec 策略配置模式	**[no] ipsec policy**
配置 tunnel 策略	**tunnel local** *<本端机构私网>* *<本端公网出口 IP>* **peer <** *总部私网>* *<总部 VPN Server IP>*
配置 pre-share-key	**isakmp pre-share-key** *<明文 PSK 字符串>*
配置 ISAKMP 本端 ID	**isakmp my-identifier** *{ip-addrl domain l email_addr}*
配置 phase-1 ISAKMP SA 加密算法	**isakmp encryption** *<加密算法>*
配置 phase-1 ISAKMP SA hash 算法	**isakmp hash** *<hash 算法>*

配置 phase-1 ISAKMP SA DH 组号	**isakmp dh-group** *<1,2,5,14-18>*
配置 phase-1 ISAKMP SA 有效期秒数	**isakmp life-time <900-86400>**
配置 phase-2 IPSEC SA 加密算法	**sa encryption** *<加密算法>*
配置 phase-2 IPSEC SA 认证校验算法	**sa authentication** *<认证校验算法>*
配置 phase-2 IPSEC SA PFS DH 组号	**sa pfs-group** *<1,2,5,14-18>*
配置 phase-2 IPSEC SA 有效期秒数	**sa life-time <900-86400>**
重启 ipsec 服务	**ipsec service restart**
查看当前 ipsec 配置	**show running-config ipsec**
查看当前 ipsec isakmp 状态	**show ipsec isakmp**
查看当前 ipsec sa 状态	**show ipsec sa**

8. pf 配置

package filter 命令用于设置进出端口的数据包的过滤规则。

说明	命令格式
过滤进出端口的 tcp/udp 数据包，并匹配源地址、源端口、目的地址、目的端口	**pf** { **pass**|**block** } { **in**|**out** } {**eth***<0-5>*|**tun***<0-3>*} {**tcp**|**udp**} **from** *src-addr1*[**/***<0-32>*] *<0-65535>* [**-***<0-65535>*] **to** { *dst-addr1*[**/***<0-32>*]|**local** } *<0-65535>* [**-***<0-65535>*]
过滤进出端口的数据包，只匹配源地址和目的地址	**pf** { **pass**|**block** } { **in**|**out** } {**eth***<0-5>*|**tun<0-3>**} **from** *src-addr2*[**/***<0-32>*] to *dst-addr2*[**/***<0-32>*]
过滤进出端口的 icmp 包，可指定 icmp 的类型(可选)：echo、echo-reply 或自定义 type code	**pf** { **pass**|**block** } { **in**|**out** } {**eth***<0-5>*|**tun<0-3>**} **icmp** **from** *src-addr3*[**/***<0-32>*] to *dst-addr3*[**/***<0-32>*] [icmp-**type** { **echo**|**echo-reply**| *<0-255>*}]
查看包过滤配置	**show running-configuration pf**
查看包过滤规则及统计	**show pf status**

dst-addr1：tcp/udp 数据包的目的 IP 地址。local 代表所有网关本身的 IP 地址。

dst-addr2：数据包的目的 IP 地址或网络号。

dst-addr3：icmp 包的目的 IP 地址或网络号。

src-addr1：tcp/udp 数据包的源 IP 地址或网络号

src-addr2：数据包的源 IP 地址或网络号

src-addr1：icmp 包的源 IP 地址或网络号

9. vrouter 及 policy-routing 配置

9.1 vrouter、route

说明	命令格式
进入 vrouter 配置模式	**vrouter** *string*
配置默认路由	**route default-gateway** *ip-addr*
建立静态路由	**router** *network mask ip-addr*
[删除]设置制定的 route zone 的下一跳	**[no] route rtzone** *name gateway*
查看路由状态	**show route** [*name* | *dst-net*]

string：vrouter 的名称。vrouter main 是默认的路由组，即没有符合其他静态和策略路由时，用户会走 vrouter main 里设置的路由。

ip-addr：下一跳的 IP 地址，即相邻路由器的接口地址。

dst-net：要查看的目的网络号

network：路由要到达的目的网络。

name：要查看的路由表名称

mask：子网掩码。

9.2 policy-routing 配置

说明	命令格式
根据源地址和目的地址条件建立策略路由	**policy-routing from** *network1/<0-32>* **to** *network2/<0-32>* **via-vrouter** *string*
根据 isp-policy-id 建立策略路由	**policy-routing isp-policy-id** *number* **via-vrouter** *string*
查看策略路由状态	**show policy-routing status**

network1：源地址网络号

network2：目的地址网络号

string：vrouter 名称

number：isp-policy-id 编号

10.bw-bonus 配置

说明	命令格式
[关闭]启用动态带宽	**[no] bw-bonus enable**
配置共享带宽的关联上行接口策略	**bw-bonus {eth<0-5> | tun<0-3>} throttle <2-500 Mbps> <2-500 Mbps > weight <0~100>**
配置每用户动态带宽上限	**bw-bonus max-per-user <1-20 Mbps> <1-20 Mbps>**
配置动态带宽分配系数	**bw-bonus factor <0.1-10>**
配置禁用动态带宽分配的区域	**bw-bonus exclude-vlan <1-4094> <1-4094>**
查看动态带宽配置	**show running-config bw-bonus**
查看最近 3 小时内的动态带宽授权历史记录	**show bw-bonus history**

11.traffic-control 配置

说明	命令格式
进入端口流控策略配置模式	**traffic-control eth[0-5] {outboundlinbound}**
配置流控策略总带宽	**total-rate <10-1000 Mbps >**
[关闭]配置 pipe 流控管道规则	**pipe <1-10> committed-rate <1-1000 Mbps > ceiling-rate <1-1000 Mbps > priority {lowest llower llowlmedium lhigh lhigher lhighest}** **no pipe <1-10>**
按协议和源目的 IP 条件指定分流管道	**[no] divert {iplgrelesplicmp} from** *src _addr* **to** *dst_addr* **via-pipe <1-10** **[no] divert {tcpludp} from** *src _addr src_port* **to** *dst_addr dst_addr* **via-pipe <1-10**
按用户带宽等级指定分流管道	**[no] divert bw-tier-id <1-7> via-pipe <1-7>**
查看当前流控配置	**show running-config traffic-control**
查看各个接口的流控状态	**show traffic-control status eth[0-5]**
清空所有的流控策略	**traffic-control flush-policy**

启用当前的流控策略	**traffic-control apply-policy**

12.vrrp 配置

说明	命令格式
[禁用]启用双机热备功能	**[no] vrrp enable**
配置网关初始状态	**vrrp init-status** *{ master l backup}*
配置 Group ID 和优先级	**vrrp group <1~15> prio <1-255>**
配置监测和随动端口	**vrrp monitor eth<0-5>**
重新启动双机热备服务	**vrrp service restart**
强制设置网关状态	**vrrp force***{ master l backup}*
查看双方主备状态	**show vrrp status**

13.show

说明	命令格式
show 命令用于显示各种配置和状态信息。"|"+ include 筛选包含关键字的信息 "|"+exclude 筛选不包含关键字的信息	**show** *command* [**l** { **include** | **exclude** } *key-word*]
查看 arp 信息，可根据 IP 和 MAC 查看	**show arp** [*ip-addr* | *mac-addr*]
查看最近 3 小时内的动态带宽授权历史记录	**show bw-bonus history**
查看指定 IP 的连接数	**show connections** *ip-addr*
查看连接数统计	**show connections statistics**
查看 DHCP 地址释放时间	**show dhcp lease** [*ip-addr*]
查看 DHCP 运行状态	**show dhcp statistics**
查看 icmp 统计信息	**show icmp statistics**
查看接口状态	**show interface statistics** [**eth***<0-5>* | **tun***<0-3>*]
查看所有 IP 接口	**show ip interface**
查看所有 IP 报文信息	**show ip statistics**
查看当前 ipsec isakmp 状态	**show ipsec isakmp**
查看当前 ipsec sa 状态	**show ipsec sa**

查看当前在线的管理员信息	**show login**
查看各个 vlan 的 MAC 数上限及状态	**show mac statistics**
列出设备 MAC 在网关中的绑定关系及状态	**show mac**
查看 MAC 过滤信息统计	**show mac filter status**
查看 MAC 地址黑名单信息	**show mac flood-list**
根据 vlan 号或 MAC 地址查看 MAC 与 Vlan 的绑定关系表	**show mac** { ***<1-4094>*** | *mac-addr* }
查看网关内存使用情况	**show memory**
查看 nat 规则及状态	**show nat status**
查看在线（直通）用户信息	**show online-user** [**trusted**]
查看在线用户统计信息	**show online-user statistics**
根据用户 IP 或 MAC 查询在线用户详细信息	**show online-user** { *ip-addr* | *mac-addr* }
根据用户账号名查询在线用户信息	**show online-user name** *uid*
查看系统自动建立的 proxy-arp 规则	**show proxy-arp**
查看包过滤规则及统计	**show pf status**
查看即插即用用户状态列表	**show i-nat**
查看即插即用的状态统计	**show i-nat statistics**
查看策略路由状态	**show policy-routing status**
查看进程[占用 cpu]的状态	**show process** [**cpu**]
查看 radius 认证统计	**show radius statistics**
查看已经通过后台认证的 MAC 地址的认证状态信息	**show radius cache** [**statistics** | *mac-addr*]
查看路由状态	**show route** [*name* | *dst-net*]
查看网关对应区块的配置	**show running-configuration** [**interface** | **route** | **access-control** | **aaa-policy** | **radius** | **arp** | **dhcp** | **nat** | **pf** | **mac** l **ipsec** l **bw-bonus** l **traffic-control**]
查看启动配置	**show startup-configuration**
查看网关本地 tcp 连接	**show tcp status**
查看 tcp 报文统计	**show tcp statistics**
查看各个接口的流控状态	**show traffic-control status eth[0-5]**
查看网关本地 udp 连接	**show udp status**
查看 udp 报文统计	**show udp statistics**
查看双方主备状态	**show vrrp status**

14.OTHER COMMANDS

14.1 arp

说明	命令格式
绑定用户的 IP 和 MAC 地址。	**arp permanent** *ip-addr mac-addr*
强制在指定 LAN 接口或所有接口进行 ARP announce	**arp announce eth<0-5>** **arp announce all-interfaces**
查看 arp 信息，可根据 IP 和 MAC 查看	**show arp** [*ip-addr* | *mac-addr*]

ip-addr：绑定的 IP 地址

mac-addr：绑定的 MAC 地址，格式：xx:xx:xx:xx:xx:xx

14.2 authorize

说明	命令格式
按 ip 授权用户上下行带宽上限，前者为上行带宽，后者为下行带宽。单位：kbps	**authorize** *ip-addr* **bandwidth** *<100-1000000>* *<100-1000000>*
按 ip 授权用户最大连接数。	**authorize** *ip-addr* **connection-limit** *<10-10000>*
对 trust 用户授权变更 name，每个 trust 用户只能改一次。	**authorize** *ip-addr* **name** *uid*
按 ip 授权用户的 isp-policy-id	**authorize** *ip-addr* **isp-policy-id** *<1-8>*
按 ip 授权用户的带宽等级	**authorize** *ip-addr* **bw-tier-id**

14.3 copy

说明	命令格式
保存配置到指定位置	**copy startup-configuration** *dst-uri*
从指定位置导入配置	**copy** *src-uri* **startup-configuration**
保存页面到指定位置	**copy portal-package** *dst-uri*
保存网关日志到指定位置	**copy syslog** *dst-uri*
上传 route zone 到网关	**copy rtzone** *src-uri name*
上传 openvpn 证书到网关	**copy** *src-uri* **openvpn-certificates**

dst-uri：目的位置的链接，可以是 tftp:// scp:// https:// http://
src-uri: 源位置的链接。
name：定义的 route zone 的名字。

14.4 configure

说明	命令格式
进入配置模式	**configure terminal**
进入快速配置模式	**configure wizard**

14.5 dns

说明	命令格式
配置主 dns 地址	dns primary *ip-addr*
配置备用 dns 地址	dns secondary *ip-addr*

ip-addr：DNS 服务器的 IP 地址

14.6 enable、exit

说明	命令格式
配置 enable 密码	enable password
退回上一级	exit

14.7 hostname

说明	命令格式
hostname 更改网关的主机名称	**hostname** *string*
cpu 均衡负载操作	**irq-balance**

string：网关主机名称

14.8 irq-balance

说明	命令格式
cpu 均衡负载操作	**irq-balance**

14.9 mac

说明	命令格式
[关闭]开启 MAC 泛洪防护功能	[no] mac anti-flood enable
设置 MAC 泛洪检测时间周期及锁住时间	mac anti-flood detect-interval *〈5-20〉* block-time *〈600-10800〉*
设置 MAC 泛洪检测周期内单个 MAC 用户建立的 arp 连接阀值	mac anti-flood threshold arp-create *〈30-300〉*
设置 MAC 泛洪检测周期内单个 MAC 用户发送的 arp 包的阀值数	mac anti-flood threshold arp-packets *〈30-1000〉*
设置 MAC 泛洪检测周期内单个用户建立链接的阀值数	mac anti-flood threshold user-create *〈20-500〉*
设置默认的每 VLAN 的 MAC 数限制	mac default-limit *num*
限制指定的 MAC 设备接入网关[可以设置绑定的接口]	mac filter block *mac-addr* [eth*〈0-5〉*]
网关对指定的 mac 地址放行，不进行黑名单探测[可以设置绑定的接口]	mac filter trust *mac-addr* [eth*〈0-5〉*]
限制指定 VLAN（或范围）内的终端 MAC 数上限	mac limit *num* vlan *〈1-4094〉 〈1-4094〉*
将指定的终端 MAC 绑定到指定的 VLAN	mac permanent *mac-addr* vlan *〈1-4094〉*
查看 MAC 对应 vlan 信息、MAC 泛洪详情，参见 7、show 命令表	show mac [statistics| filter| flood-list| *〈1-4094〉* | *mac-addr*]

14.10 man

说明	命令格式
解释命令语句的用法	man *command*

command：命令语句

14.11 ping

说明	命令格式
Ping 测试命令	Ping *ip_addr*

ip-addr：需要测试的 IP 地址

14.12 portal

说明	命令格式
重启 portal 相关服务	**Portal service restart**
第三方 portal 认证 URL	**[no]portal third-party auth-url URL**
第三方 portal 计费 URL	**[no]portal third-party acct-url URL**
第三方 portal 在线监测 URL	**[no]portal third-party keep-alive-url URL**

14.13 remove

说明	命令格式
清除 arp 表中对应地址	**remove arp** *ip-addr*
清除 MAC 黑名单中对应地址	**remove mac flood-list** *mac-addr*
删除 MAC 对应 vlan 的信息，注意固定的对应记录也会被删除。	**remove mac** *mac-addr* **vlan** *〈1-4094〉*
踢在线用户下线，并删除对应的 radius cache	**remove online-user** { *ip-addr* | *mac-addr* }
删除 openvpn 证书	**remove openvpn-certificates**
删除 route zone	**remove rtzone**
删除 radius cache 中对应记录	**remove radius-cache** *mac-addr*
踢对应 pid 的管理员账号下线	**remove login** *pid*
重启 portal 相关服务	**portal-service restart**

ip-addr：需要测试的 IP 地址

mac-addr：对应的 MAC 地址

14.14 trace-route

说明	命令格式
命令用于测试跟踪数据包经过的路由及节点信息	trace-route { *website* | *ip-addr* }

website：需要测试的网站域名或主机名

14.15 terminal

说明	命令格式
设置登陆超时时间	**terminal timeout** *〈180-900〉*

14.16 tcpdump

说明	命令格式
[根据 ip 或 mac 地址]抓包并上传到指定位置。	**tcpdump eth***<0-5>* [**match** { *ip-addr* | *mac-addr* }] **upload** *dst-uri*

ip-addr：抓包指定的 ip 地址。
mac-addr：抓包指定的 mac 地址。
dst-uri：抓包后文件上传的位置。可以是 tftp、scp，如果有密码，上传时会提示输入密码。

14.17 netflow

说明	命令格式
[关闭]开启上网日志	[no] netflow enable
[关闭]开启公安审计功能	[no] netflow gat-695-audit enable
设置上网日志每秒记录的最大日志数量	netflow rate-limit *〈500-5000〉*
上网日志忽略[不忽略]DNS 协议或未建立成功的 TCP 连接或 lan 相关协议	[no] netflow skip { dns-protocol |half-tcp-connection | lan-protocol }

14.18 user、

说明	命令格式
创建或修改网关管理员账号和密码。 带 local-auth 选项的账号同时可以作为本地认证账号使用。	user *name* password *passwd* [local-auth]

name：用户名。

passwd：密码，非本地账号的密码在配置中显示为加密的文字。

14.19 write

说明	命令格式
保存，将 running-config 写入到 startup-config	Write