

# 云路由设备使用手册

## 目录

1.1	登录 WebUI 配置界面 .....	3
1.2	登录 WebUI 配置界面 .....	3
1.2	状态 .....	4
1.2.1	总览 .....	4
1.2.3	路由表 .....	6
1.2.4	实时信息 .....	7
1.2.4.1	CPU 负载 .....	7
1.2.4.2	实时流量 .....	8
1.3	系统 .....	9
1.3.1	系统 .....	9
1.3.2	管理权 .....	9
1.3.3	备份/升级 .....	10
1.4	网络 .....	11
1.4.1	接口 .....	11
1.4.1.1	配置 lan 口 .....	11
1.4.1.2	配置 wan 口 .....	12
1.4.2	交换机 (S 系列) .....	14
1.4.3	DHCP/DNS .....	15
1.4.3.1	DNS 转发 .....	15

1.4.3.2 IP/MAC 绑定.....	17
1.4.4 主机名.....	18
1.4.5 静态路由.....	19
1.4.6 网络诊断.....	20
1.4.7 防火墙.....	20
1.4.7.1 基本配置.....	21
1.4.7.2 区域.....	22
1.4.7.3 端口转发.....	25
1.4.7.4 通信策略.....	26
1.4.8 SNMP.....	30
<b>1.5 流量整形使用规则 (EH 系列)</b> .....	<b>31</b>
1.5.1 流量整形.....	31
1.5.2 地址与域名.....	32
1.5.3 接口与共享带宽组.....	33
1.5.4 共享带宽规则.....	34
1.5.7 Per IP 限速规则.....	34
1.5.6 Per IP 限速规则配置范例.....	35
1.5.8 共享带宽规则配置范例.....	36

## 1.1 登录 shell 配置界面

登录方式 ssh/console，端口号为 28822

登录账号:root

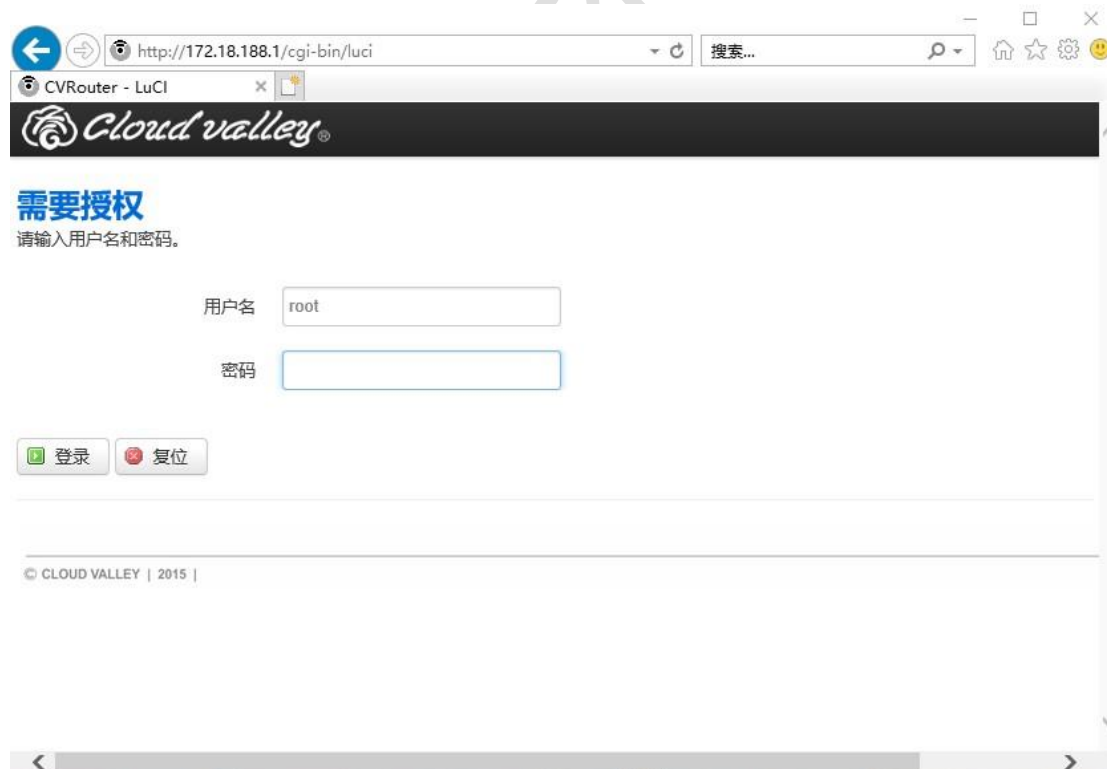
密 码:root

支持 mtr,iftop,iperf3,ping 等命令

## 1.2 登录 WebUI 配置界面

电脑直连云设备 lan 口，通过 Web 界面来配置云设备，方法如下：

首先电脑需配置为自动获取 ip（默认获取到 172.18.188.X/24），然后在浏览器中输入云设备的默认登录 IP，输入 172.18.188.1，页面如下：



在登录

框输入『用户名』和『密码』，点击登录按钮即可登录云设备进行配置，

默认情况下的用户名和密码均为：root。



登录 WebUI 配置界面后，可以看到有以下配置内容：

『状态』：用来查看当前设备的运行状态

『系统』：配置云设备的基本信息及查看网关运行的基本状态等

『网络』：配置云设备的网口及相关网络配置

『退出』：退出配置界面

## 1.2 状态

『状态』包含『总览』、『防火墙』、『路由表』、『实时信息』、等子模块。

### 1.2.1 总览

总览中可以查看当前设备运行状态，包括内存占用率、wan 口网关地址、设备固件版本、设备运行时间等，页面如下：

Cloud valley   状态   系统   网络   退出

---

主机型号	CVR S800
固件版本	CVROS S800 1.4.5
内核版本	3.10.14
本地时间	Tue Jan 22 10:09:19 2019
运行时间	1h 42m 45s
平均负载	0.00, 0.03, 0.05
认证	Yes

### 内存

可用数	93628 kB / 125284 kB (74%)
空闲数	73400 kB / 125284 kB (58%)
已缓存	15228 kB / 125284 kB (12%)
已缓冲	5000 kB / 125284 kB (3%)

### 网络

IPv4 WAN状态

类型:	dhcp
eth1 地址:	172.18.100.187
子网掩码:	255.255.255.0
网关:	172.18.100.1
DNS 1:	172.18.100.1
已连接:	1h 42m 27s

## 1.2.2 防火墙

用于查看每条防火墙规则所匹配的流量数据总量

### 防火墙状态

IPv4 防火墙 IPv6 防火墙

表: Filter

复位计数器

重启防火墙

链 INPUT (策略: ACCEPT, 数据包: 0, 流量: 0.00 B)

数据包	流量	目标	协议	入口	出口	源地址	目标地址	选项
9911	884.05 KB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	! fw3 */
155570	55.87 MB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	! fw3: Custom input rule chain */
120200	52.73 MB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED ! fw3 */
88	4.69 KB	syn_flood	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02 ! fw3 */
0	0.00 B	zone_lan_input	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	! fw3 */
402	515.30 KB	zone_wan_input	all	eth0.2	*	0.0.0.0/0	0.0.0.0/0	! fw3 */
34968	2.63 MB	zone_vpn_input	all	tap1	*	0.0.0.0/0	0.0.0.0/0	! fw3 */
0	0.00 B	zone_vpn_input	all	tap2	*	0.0.0.0/0	0.0.0.0/0	! fw3 */

链 FORWARD (策略: DROP, 数据包: 0, 流量: 0.00 B)

数据包	流量	目标	协议	入口	出口	源地址	目标地址	选项
97	10.93 KB	qos_forwarding	all	*	*	0.0.0.0/0	0.0.0.0/0	-
97	10.93 KB	forwarding_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	! fw3: Custom forwarding rule chain */
0	0.00 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED ! fw3 */
0	0.00 B	zone_lan_forward	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	! fw3 */
0	0.00 B	zone_wan_forward	all	eth0.2	*	0.0.0.0/0	0.0.0.0/0	! fw3 */
97	10.93 KB	zone_vpn_forward	all	tap1	*	0.0.0.0/0	0.0.0.0/0	! fw3 */

## 1.2.3 路由表

路由表可以查看云设备的 ARP 表,IPv4-链路表以及 IPv6-链路表, 页面如

下:

Cloud valley   状态   系统   网络   退出

### 路由表

系统中的活跃连接。

#### ARP

IPv4-地址	MAC-地址	接口
172.18.100.1	b0:51:8e:04:9b:e8b	eth1
172.18.100.50	00:11:32:80:6e:a0	eth1
172.18.188.101	48:45:20:c6:e7:89	br-lan
172.18.100.14	3a:afef:1c:da:c5	eth1

#### 活动的IPv4-链路

网络	目标	IPv4-网关	跃点数	表
vpn	0.0.0.0/0		0	main
vpn	103.208.189.224/27		0	main
wan	172.18.100.0/24		0	main
lan	172.18.188.0/24		0	main

#### 活动的IPv6-链路

网络	目标	源地址	跃点数	表
wan	:::1		0	local

## 1.2.4 实时信息

实时信息用于查看设备的 CPU 负载以及设备的各个接口的流量情况。

### 1.2.4.1 CPU 负载

设备的 cpu 负载峰值为 4，负载低于 3 时属于正常情况。若负载超过 3 或者接近 3 时，需联系我方技术人员排查。页面如下：



## 1.2.4.2 实时流量

其中, eth0.1 为 lan 口的流量, eth0.2 为 wan 口的流量, tap 为组网的流量。各个接口的流量如下:





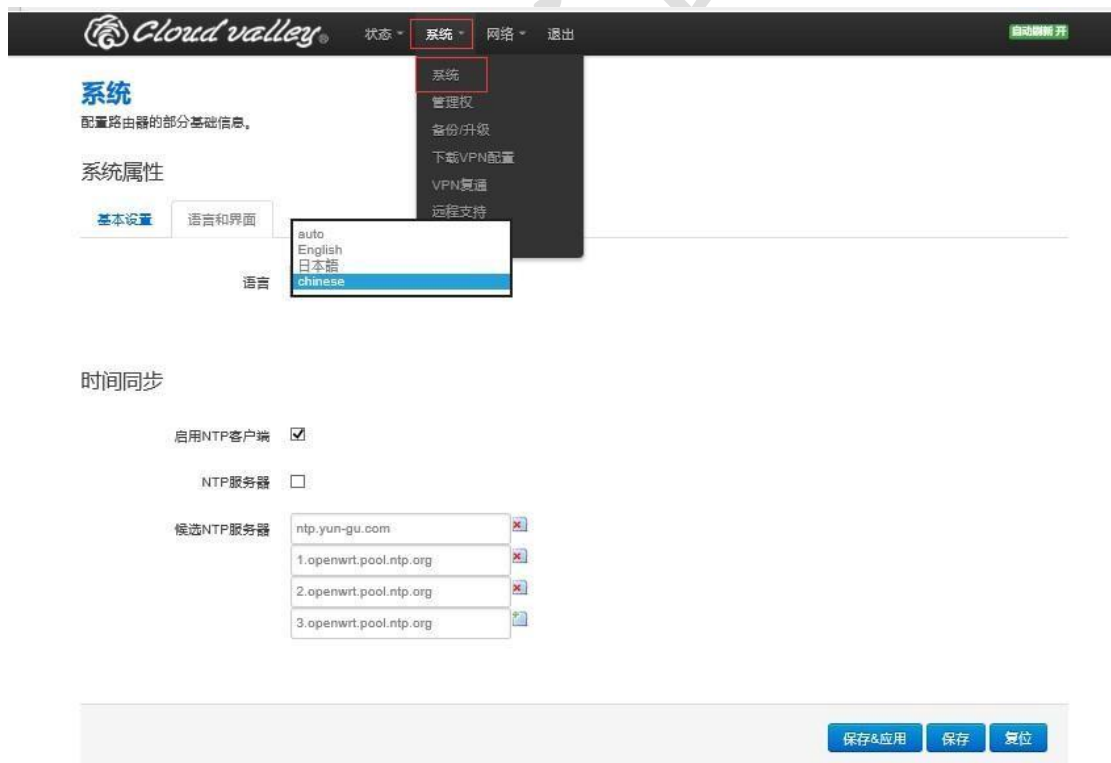
其中入站是指下载数据的流量情况，在图中用蓝色的线表示。出站是指上传数据的流量情况，在图中用绿色的线表示。

## 1.3 系统

『系统』包含『系统』、『管理权』、『备份/升级』、『重启』等子模块。

### 1.3.1 系统

用于设置时间同步以及设置界面显示的语言，其中语言默认是中文，可以选择英语、日语。页面如下：



### 1.3.2 管理权

用于修改 WebUI 配置界面的登陆密码，页面如下：



### 1.3.3 备份/升级

用于恢复出厂设置，备份配置的信息，升级固件。其中升级固件时，若版本跨度过大，先把保留配置的勾去掉，再升级固件。页面如下：



## 1.4 网络

『网络』包含『接口』、『DHCP/DNS』、『主机名』、『静态路由』、『网络诊断』、『防火墙』、等子模块。EH 系列有『流量整形』模块

### 1.4.1 接口

用于配置 lan 口，wan 口以及查看组网口的运行信息。页面如下：



Cloud valley 荟谷 状态 系统 网络 退出 自动重新打开

### 接口

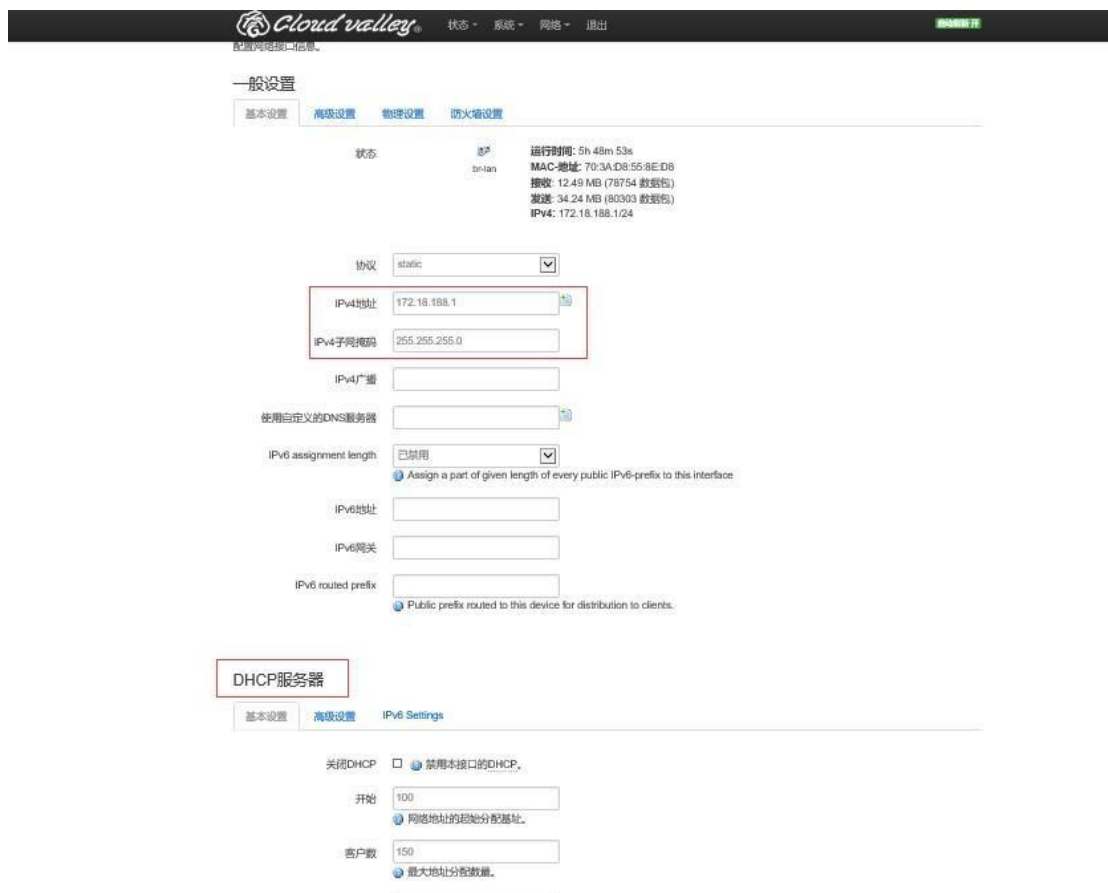
接口总览

网络	状态
<b>LAN</b> br-lan	运行时间: 5h 46m 55s MAC-地址: 70:3A:D8:55:8E:D8 接收: 12.43 MB (78167 数据包) 发送: 34.10 MB (79718 数据包) IPv4: 172.18.188.1/24
<b>VPN</b> tun0	运行时间: 5h 46m 21s MAC-地址: 00:00:00:00:00:00 接收: 15.79 MB (31222 数据包) 发送: 6.50 MB (29484 数据包) IPv4: 103.206.189.227/27
<b>WAN</b> eth1	运行时间: 5h 46m 49s MAC-地址: 70:3A:D8:55:8E:D9 接收: 47.55 MB (144496 数据包) 发送: 13.87 MB (70425 数据包) IPv4: 172.18.100.187/24

添加新接口...

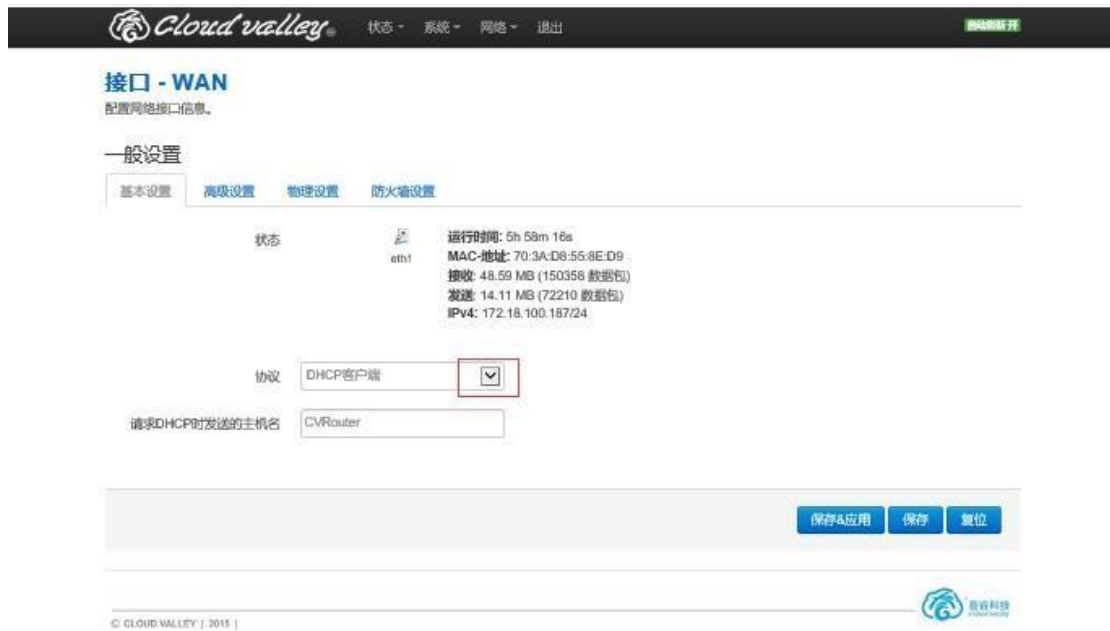
#### 1.4.1.1 配置 lan 口

lan 口的 IP 可以自定义修改，以及配置 dhcp。点击修改后，页面如下：



### 1.4.1.2 配置 wan 口

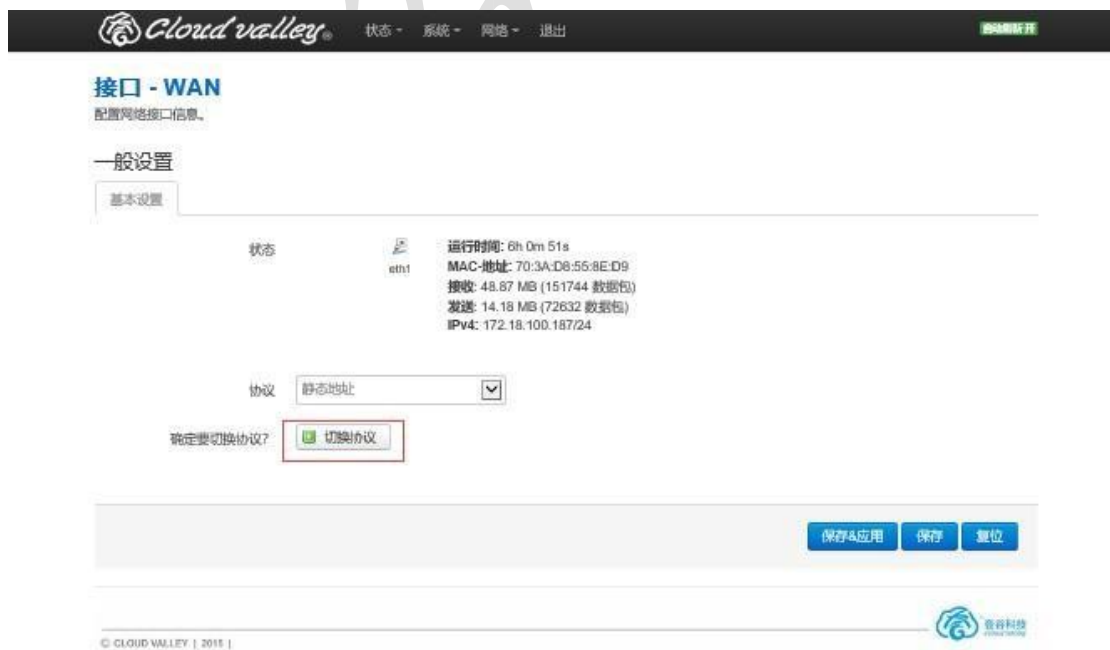
wan 口可以支持 pppoe、静态 ip、DHCP 客户端以及 DHCPV6 客户端。wan 口默认是 dhcp 客户端的，下面介绍 wan 口如何切换成其他模式，以切换为静态地址为例。点击 wan 口的修改后，页面如下：



The screenshot shows the '接口 - WAN' (WAN Interface) configuration page. Under the '一般设置' (General Settings) tab, the '协议' (Protocol) dropdown menu is set to 'DHCP客户端' (DHCP Client). The '请求DHCP时发送的主机名' (Host name sent when requesting DHCP) field contains 'CVRouter'. The status section shows the interface 'eth1' is up, with a runtime of 5h 59m 16s, MAC address 70:3A:D6:55:8E:D9, and IPv4 address 172.18.100.187/24. At the bottom right, there are buttons for '保存&应用' (Save & Apply), '保存' (Save), and '复位' (Reset).

点击红

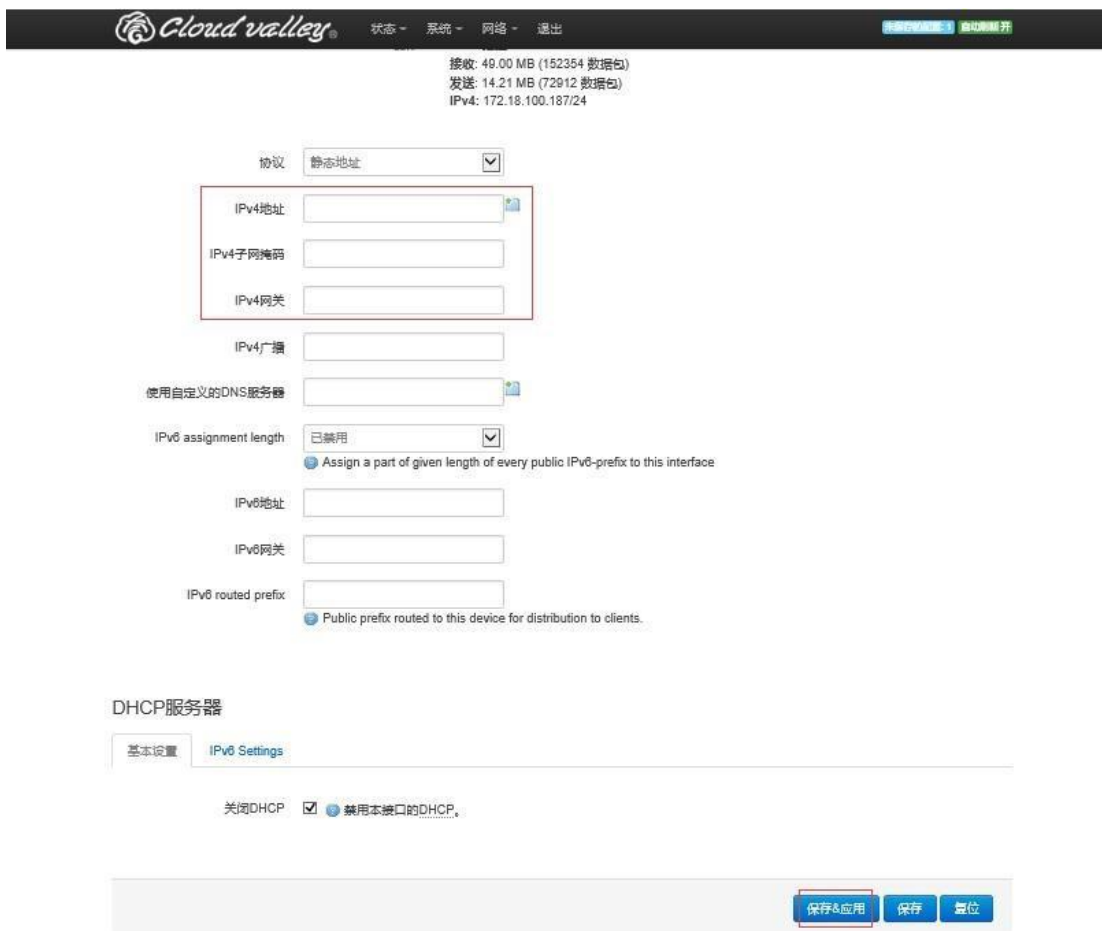
框，并选择静态地址后，页面如下：



The screenshot shows the '接口 - WAN' (WAN Interface) configuration page with the '协议' (Protocol) dropdown menu set to '静态地址' (Static IP). A '切换协议?' (Switch Protocol?) dialog box is displayed, with a red box highlighting the '切换协议' (Switch Protocol) button. The status section shows the interface 'eth1' is up, with a runtime of 6h 0m 51s, MAC address 70:3A:D6:55:8E:D9, and IPv4 address 172.18.100.187/24. At the bottom right, there are buttons for '保存&应用' (Save & Apply), '保存' (Save), and '复位' (Reset).

点击切换

协议，便可切换到静态地址模式。页面如下：




The screenshot shows a network configuration page for Cloud Valley. At the top, there is a navigation bar with 'Cloud valley' logo and links for '状态', '系统', '网络', and '退出'. Below the navigation bar, there is a status bar showing network statistics: '接收: 48.00 MB (152354 数据包)', '发送: 14.21 MB (72912 数据包)', and 'IPv4: 172.18.100.187/24'. The main configuration area is titled '协议' (Protocol) and is set to '静态地址' (Static Address). It contains several input fields: 'IPv4地址' (IPv4 Address), 'IPv4子网掩码' (IPv4 Subnet Mask), 'IPv4网关' (IPv4 Gateway), 'IPv4广播' (IPv4 Broadcast), '使用自定义的DNS服务器' (Use custom DNS server), 'IPv6 assignment length' (set to '已禁用'), 'IPv6地址' (IPv6 Address), 'IPv6网关' (IPv6 Gateway), and 'IPv6 routed prefix'. Below this is a section for 'DHCP服务器' (DHCP Server) with a sub-tab 'IPv6 Settings'. It includes a checkbox for '禁用本接口的DHCP' (Disable DHCP on this interface) which is checked. At the bottom right, there are three buttons: '保存&应用' (Save & Apply), '保存' (Save), and '复位' (Reset).

填写对应的 ip 信息，并保存&应用便可生效。

## 1.4.2 交换机 (S 系列)

本设备可以划分为多个 VLAN，并支持电脑间的直接通讯。VLAN 也常用于分割不同网段。默认通常是一条上行端口连接 ISP，其余端口为本地子网。

 状态 ▾ 系统 ▾ 网络 ▾ 退出 自动刷新







### 交换机


本设备可以划分为多个 VLAN，并支持电脑间的直接通讯。VLAN 也常用于分割不同网段。默认通常是一条上行端口连接 ISP，其余端口为本地子网。

交换机 "switch0" (mt7530)

启用 VLAN

#### "switch0" (mt7530) 上的 VLAN

VLAN ID	CPU (eth0)	LAN 4	LAN 3	LAN 2	LAN 1	WAN	动作
端口状态:	 1000baseT 全双工	 未连接	 未连接	 未连接	 未连接	 1000baseT 全双工	
1	已标记 ▾	未标记 ▾	未标记 ▾	未标记 ▾	未标记 ▾	关 ▾	删除
2	已标记 ▾	关 ▾	关 ▾	关 ▾	关 ▾	未标记 ▾	删除

© CLOUD VALLEY | 2020 | 

## 1.4.3 DHCP/DNS

用于设置 DHCP 配置、DNS 配置，以及 IP/MAC 绑定。如查看已分配的 DHCP 租约，设置 dns 转发等配置。

### 1.4.3.1 DNS 转发

主要用于某些域名需要用到特定的 dns 服务器解释，例如私有的域名或者其他需要指定 DNS 服务器解释的域名等。页面如下：

服务器设置

基本设置

高级设置

唯一授权  
这是本地网络中唯一的 DHCP 服务器

本地服务器   
本地域名规则。与此域匹配的名称从不转发，仅从 DHCP 或 HOSTS 文件解析

本地域名   
本地域名后缀将添加到 DHCP 和 HOSTS 文件条目

DNS 转发

<input type="text" value="/example.org/10.1.2.3"/>	<input type="button" value="x"/>
<input type="text" value="/baidu.com/114.114.114.114"/>	<input type="button" value="+"/>

将请求转发到的 DNS 服务器列表

重绑定保护  
丢弃 RFC1918 上行响应数据

允许本机  
允许 127.0.0.0/8 回环范围内的上行响应，例如：RBL 服务

域名白名单    
允许 RFC1918 响应的域名列表

仅本地服务  
仅在网卡所属的子网中提供 DNS 服务。

非全部地址  
仅绑定到特定接口，而不是全部地址。

监听接口    
仅监听这些接口和环回接口。

排除接口    
不监听这些接口。

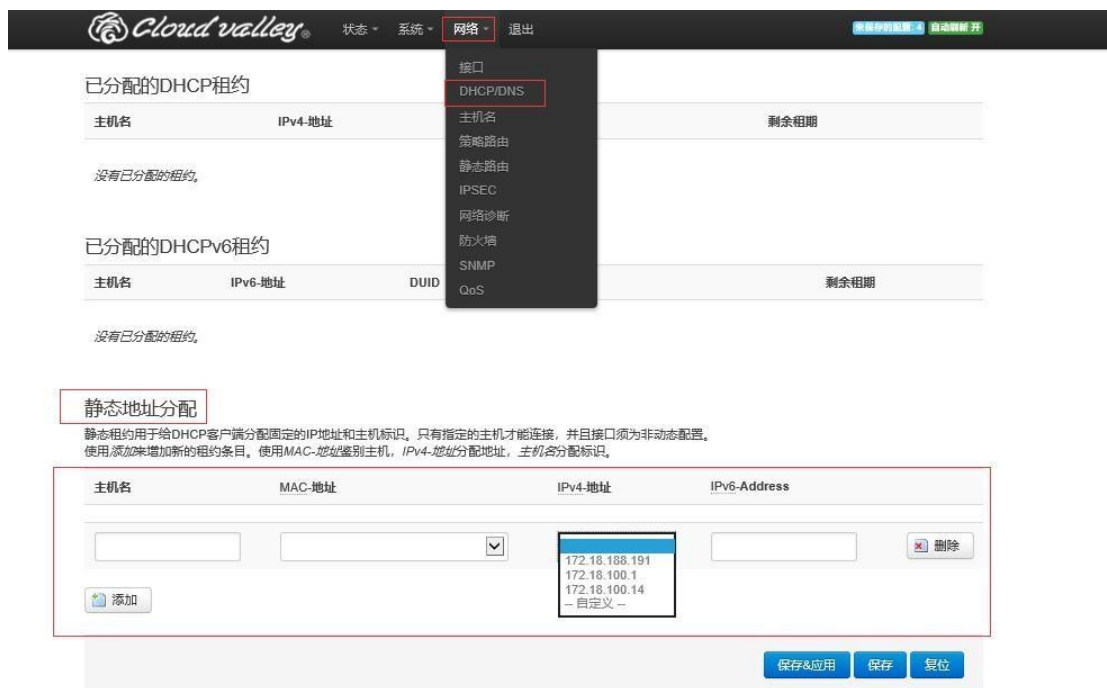
云设备支持自定义 dns 服务器的端口和最大并发查询数，页面如下：





### 1.4.3.2 IP/MAC 绑定

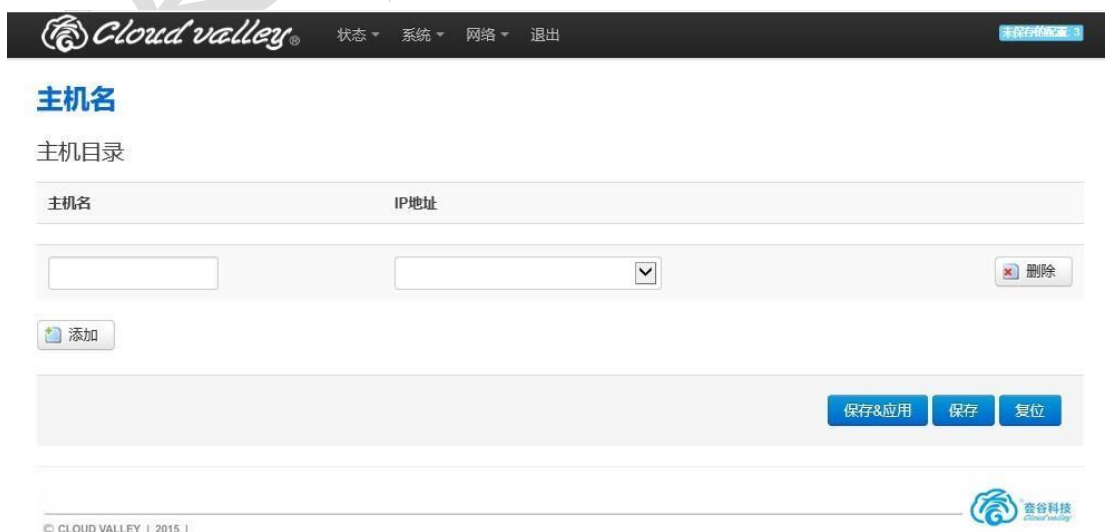
云设备提供了“IP/MAC 绑定”功能，通过此功能可以自动搜索内网 IP 地址所对应的 MAC 地址并将它们绑定在一起，当局域网内部有未知设备接入时，由于在 IP/MAC 绑定表中没有它的记录，未知设备将无法通过云设备网关上网。当某个 IP 所对应的 MAC 地址与记录不符时，云设备也将拒绝此 IP 的上网请求，页面如下：



The screenshot shows the 'Network' section of the Cloud Valley management interface. It features two tables for DHCP leases (IPv4 and IPv6) and a 'Static IP Address Allocation' form. The form includes fields for Host Name, MAC Address, IPv4 Address, and IPv6 Address, along with a dropdown menu for IP addresses and buttons for 'Add', 'Save & Apply', 'Save', and 'Reset'.

## 1.4.4 主机名

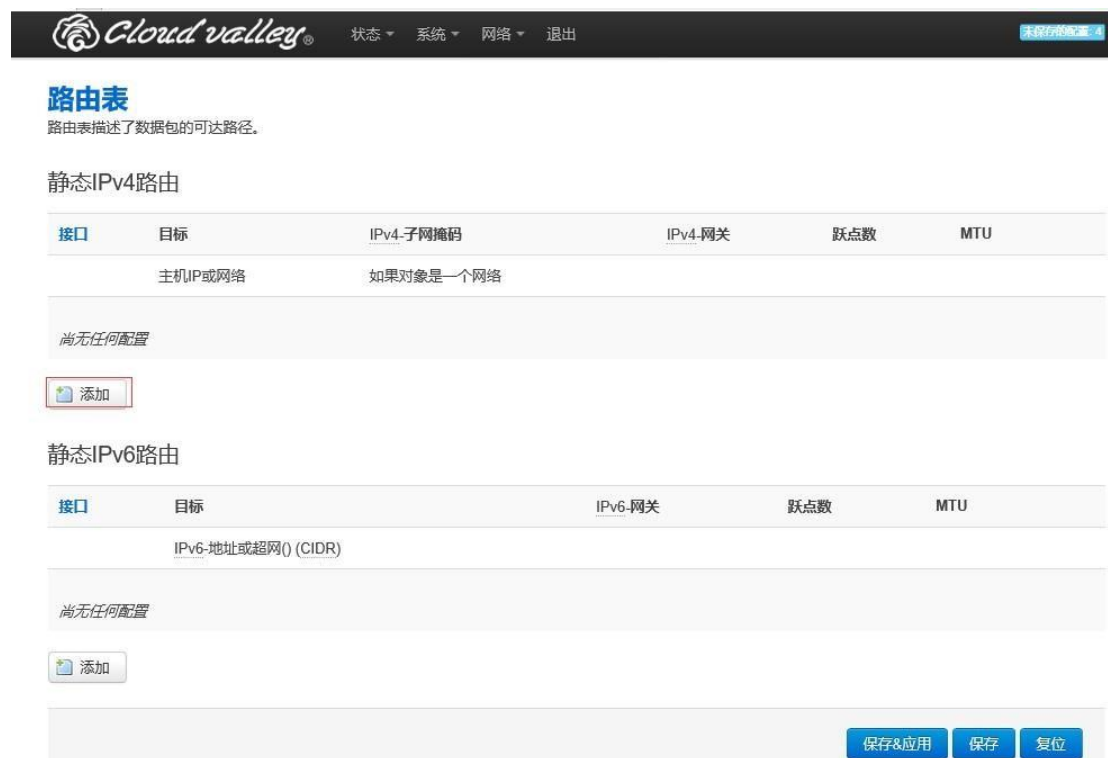
用于绑定域名与 ip, 页面如下:



The screenshot displays the 'Host Name' configuration page. It includes a header with the Cloud Valley logo and navigation menu. The main content area is titled 'Host Name' and 'Host Name Directory'. It features a table with columns for 'Host Name' and 'IP Address', and a form below with input fields and a dropdown menu. At the bottom, there are buttons for 'Add', 'Save & Apply', 'Save', and 'Reset'.

## 1.4.5 静态路由

用于指定经过云设备某些网段或 ip 的路由走向，云设备可以设置 IPv4 以及 IPv6 的静态路由。页面如下：



**路由表**  
路由表描述了数据包的可达路径。

静态IPv4路由

接口	目标	IPv4-子网掩码	IPv4-网关	跃点数	MTU
	主机IP或网络	如果对象是一个网络			

尚无任何配置

添加

静态IPv6路由

接口	目标	IPv6-网关	跃点数	MTU
	IPv6-地址或超网() (CIDR)			

尚无任何配置

添加

保存&应用 保存 复位

点击添

加后，便可设置静态路由，其中，云设备配置静态路由，需要选择对应的接口，必须填上目标，掩码以及网关。跃点数以及 MTU 可以根据需要配置，默认留空便可。例如需要 8.8.8.8 走 wan 口出去，接口选择 wan 口，网关为 wan 口的网关。页面如下：

## 路由表

路由表描述了数据包的可达路径。

### 静态IPv4路由

接口	目标	IPv4-子网掩码	IPv4-网关	跃点数	MTU	
主机IP或网络		如果对象是一个网络				
wan	8.8.8.8	255.255.255.255	172.18.100.1	0	1500	删除

添加

### 静态IPv6路由

接口	目标	IPv6-网关	跃点数	MTU
IPv6-地址或超网() (CIDR)				
尚无任何配置				

添加

保存&应用 保存 复位

注意,

若需要配置到 lan 口的静态路由, 防火墙需要开启允许 wan 区域转发到 lan 区域, 在下面介绍防火墙的区域时会详细说明。

## 1.4.6 网络诊断

用于诊断设备的网络问题, 有 ping, traceroute, 以及 nslookup 等功能。



## 1.4.7 防火墙

云设备防火墙主要包含基本配置, 区域, 端口转发以及通信规则。

基本配置包含：防 dos 攻击，dns 劫持。

区域包含：nat 设置，设备不同区域过滤规则设置等功能。

端口转发：用于设置端口的转发通信规则：用于设置特定的通信规则。

## 1.4.7.1 基本配置

### 1.4.7.1.1 防 dos 攻击

云设备集成了高性能的企业级状态检测防火墙，能有效保护内网的部网络免受来自包括 Internet 及其它局域网等多方面的攻击。同时，内置的防 DOS 攻击功能，不仅可以有效防范来自外部网络的 DOS 攻击，对于内网计算机发起的 DOS 攻击，云设备也可以进行防御。把启用 SYN-flood 防御勾上就可以，默认时开启的。页面如下：



The screenshot shows the Cloud Valley web management interface. At the top, there is a navigation bar with 'Cloud valley' logo, '状态', '系统', '网络', and '退出'. Below the navigation bar, there are three tabs: '基本设置', '端口转发', and '通信规则'. The main content area is titled '防火墙-区域设置' (Firewall - Area Settings) with a subtitle '防火墙把网络接口分为不同的区域进行管理'. Under the '基本设置' (Basic Settings) section, there are several configuration options:

- 启用SYN-flood防御
- 丢弃无效数据包
- DNS劫持
- 入站数据: 拒绝
- 出站数据: 拒绝
- 转发: 拒绝

The '网络' (Network) menu is open, showing a list of options: 接口, DHCP/DNS, 主机名, 策略路由, 静态路由, IPSEC, 网络诊断, 防火墙 (highlighted), SNMP, and QoS.

### 1.4.8.1.1 dns 劫持

用于劫持云设备下方设备的 dns，强制使用云设备的 dns 解释，勾上 dns 劫持并保存应用便可生效。页面如下：



The screenshot shows the 'Firewall Area Settings' (防火墙-区域设置) configuration page. It has three tabs: 'Basic Settings' (基本设置), 'Port Forwarding' (端口转发), and 'Communication Rules' (通信规则). The 'Basic Settings' tab is active. Under the sub-heading 'Basic Settings' (基本设置), there are several options: 'Enable SYN-flood defense' (启用SYN-flood防御) is checked; 'Discard invalid packets' (丢弃无效数据包) is unchecked; 'DNS hijacking' (DNS劫持) is checked and highlighted with a red box; 'Inbound data' (入站数据) is set to 'Deny' (拒绝); 'Outbound data' (出站数据) is set to 'Deny' (拒绝); and 'Forwarding' (转发) is set to 'Deny' (拒绝). A large watermark '云谷' is visible in the background of the screenshot.

## 1.4.7.2 区域

### 1.4.7.2.1 NAT 设置

在云设备，IP 动态伪装是指 NAT 功能，用于设置防火墙代理局域网上网的规则，设备缺省配置 wan 口以及 vpn 口已开启 dnat，页面如下：

### 区域

区域 → 转发	入站数据	出站数据	转发	IP动态伪装	MSS钳制	
lan: lan: ⇒ wan vpn ipsec	接受	接受	接受	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">修改</a> <a href="#">删除</a>
wan: wan: ⇒ REJECT	拒绝	接受	拒绝	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">修改</a> <a href="#">删除</a>
vpn: vpn: ⇒ REJECT	拒绝	接受	拒绝	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">修改</a> <a href="#">删除</a>
ipsec: (空) ⇒ REJECT	拒绝	接受	拒绝	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">修改</a> <a href="#">删除</a>

## 1.4.7.2.2 不同区域过滤规则

主要包括 lan 区域，wan 区域，vpn 区域以及 ipsec 之间的过滤规则。默认是 lan 区域可以到达 wan，vpn，ipsec 区域。而其他区域无法到达 lan 区域。页面如下：

### 区域

区域 → 转发	入站数据	出站数据	转发	IP动态伪装	MSS钳制	
lan: lan: ⇒ wan vpn ipsec	接受	接受	接受	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">修改</a> <a href="#">删除</a>
wan: wan: ⇒ REJECT	拒绝	接受	拒绝	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">修改</a> <a href="#">删除</a>
vpn: vpn: ⇒ REJECT	拒绝	接受	拒绝	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">修改</a> <a href="#">删除</a>
ipsec: (空) ⇒ REJECT	拒绝	接受	拒绝	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">修改</a> <a href="#">删除</a>

点击修改，可以自定义wan区域的过滤规则。

下面

演示分别演示 wan 区域允许转发到 lan 区域、wan 区域允许转发到 vpn 区域。 wan 区域允许转发到 lan 区域：一般用于云设备级连方案，静态路由指向 lan 区域，以及端口转发到 lan 区域。操作如下：

点击 wan 区域右边的修改，默认转发到目的区域为空的，勾上 lan 口便可，页面如下：

#### 端口触发

以下选项可以控制区域(wan)和其它区域间的转发规则。目标区域接收从“wan”转发的流量，源区域匹配从目标为“wan”的区域的需转发流量。以下规则无法转发例如：转发lan流量到wan，但是不允许从wan转发到lan。

允许转发到目标区域

ipsec: (空)

lan: lan: 

vpn: vpn: 

允许从源区域转发

ipsec: (空)

lan: lan: 

vpn: vpn: 

[返回至概况](#) [保存&应用](#) [保存](#) [复位](#)

保存应用并

返回防火墙主页，页面如下：

#### 区域

区域 → 转发	入站数据	出站数据	转发	IP动态伪装	MSS钳制	
lan: lan:  ⇒ vpn ipsec wan	接受	接受	接受	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">修改</a> <a href="#">删除</a>
wan: wan:  ⇒ lan	拒绝	接受	拒绝	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">修改</a> <a href="#">删除</a>
vpn: vpn:  ⇒ REJECT	拒绝	接受	拒绝	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">修改</a> <a href="#">删除</a>
ipsec: (空) ⇒ REJECT	拒绝	接受	拒绝	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">修改</a> <a href="#">删除</a>

[添加](#)

同时要把入站数据与转发的拒绝选为接受。页面如下：

#### 区域

区域 → 转发	入站数据	出站数据	转发	IP动态伪装	MSS钳制	
lan: lan:  ⇒ vpn ipsec wan	接受	接受	接受	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">修改</a> <a href="#">删除</a>
wan: wan:  ⇒ lan	接受	接受	接受	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">修改</a> <a href="#">删除</a>
vpn: vpn:  ⇒ REJECT	拒绝	接受	拒绝	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">修改</a> <a href="#">删除</a>
ipsec: (空) ⇒ REJECT	拒绝	接受	拒绝	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">修改</a> <a href="#">删除</a>

[添加](#)

wan 区域允许转发到 vpn 区域：一般用于云设备单臂方案等。操作如下：



点击 wan 区域右边的修改, 默认转发到目的区域为空的, 勾上 vpn 区域便可, 页面如下:

**端口转发**

以下选项可以控制区域(wan)和其它区域间的转发规则。目标区域接收从"wan"转发的流量。源区域匹配从目标为"wan"的区域的需转发流量。以下规则无法转发, 例如: 转发lan流量到wan, 但是不允许从wan转发到lan。

允许转发到目标区域

- ipsec: (空)
- lan: lan:
- vpn: vpn:

允许从源区域转发

- ipsec: (空)
- lan: lan:
- vpn: vpn:

返回至概况      保存&应用   保存   复位

同时需

要把入站数据与转发的拒绝选为接受, 页面如下:

**区域**

区域 → 转发	入站数据	出站数据	转发	IP动态伪装	MSS钳制	
lan: lan: ⇒ vpn ipsec wan	接受	接受	接受	<input type="checkbox"/>	<input type="checkbox"/>	修改 删除
wan: wan: ⇒ vpn	接受	接受	接受	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	修改 删除
vpn: vpn: ⇒ REJECT	拒绝	接受	拒绝	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	修改 删除
ipsec: (空) ⇒ REJECT	拒绝	接受	拒绝	<input type="checkbox"/>	<input type="checkbox"/>	修改 删除

### 1.4.7.3 端口转发

用于设置云设备的 DNAT 规则, 如果局域网内的服务器需要向外网提供服务, 则需要添加端口转发设置, 页面如下:

基本设置 端口转发 通信规则

### 防火墙 - 端口转发

端口转发允许来自Internet的计算机访问私有局域网内的计算机或服务

端口转发

名 字	匹配规则	转发到	开 启	排 序
尚无任何配置				

新建端口转发:

名字	协议	外部区域	外部端口	内部区域	内部IP地址	内部端口	
新建端口转发	TCP+UDP	ipse		ipse			添加

保存&应用 保存 复位

如需要

通过 vpn 区域的 22 端口访问 lan 区域的服务器 172.18.188.2 的 22 端口。需要填上端口转发的名字，协议，选择 vpn 区域，外部端口，选择 lan 区域，内部端口，填写完毕后，必须点击添加。页面如下：

基本设置 端口转发 通信规则

### 防火墙 - 端口转发

端口转发允许来自Internet的计算机访问私有局域网内的计算机或服务

端口转发

名 字	匹配规则	转发到	开 启	排 序
尚无任何配置				

新建端口转发:

名字	协议	外部区域	外部端口	内部区域	内部IP地址	内部端口	
vpn22	TCP	vpn	22	lan	172.18.188.2	22	添加

配置完，点击添加生效

最后保存应用 ← 保存&应用 保存 复位

## 1.4.7.4 通信策略

用于不同区域间的流量传送，例如：拒绝一些主机之间的通信，打开到某些区域的端口。页面如下：

基本设置 端口转发 通信规则

### 防火墙 - 通信规则

通信规则定义了不同区域间的流量传送，例如：拒绝一些主机之间的通信、打开到WAN的端口。

通信规则

名字	匹配规则	动作	开启	排序
Allow-DHCP-Renew	IPv4-UDP 来自 所有主机 位于 wan 到 所有路由器地址 at 端口 68 位于本设备	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="修改"/> <input type="button" value="删除"/>
Allow-Ping	IPv4-ICMP 和 type echo-request 来自 所有主机 位于 wan 到 所有路由器地址 位于本设备	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="修改"/> <input type="button" value="删除"/>
Allow-DHCPv6	IPv6-UDP 来自 IP range fe80::/10 位于 wan 带宽 端口 547 到 IP range fe80::/10 at 端口 546 位于本设备	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="修改"/> <input type="button" value="删除"/>
Allow-ICMPv6-Input	IPv6-ICMP 和 types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement 来自 所有主机 位于 wan 到 所有路由器地址 位于本设备	Accept input 并且限制到 1000 包 每 second	<input checked="" type="checkbox"/>	<input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="修改"/> <input type="button" value="删除"/>
Allow-ICMPv6-Forward	IPv6-ICMP 和 types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type 来自 所有主机 位于 wan 到 所有主机 位于 所有区域	Accept forward 并且限制到 1000 包 每 second	<input checked="" type="checkbox"/>	<input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="修改"/> <input type="button" value="删除"/>

打开路由器端口:

名字	协议	外部端口
SSH	TCP	22

### 1.4.8.4.1 开放某区域的某个外部端口

云设备支持自定义不同区域的规则，例如开放 vpn 区域的外部 80 端口，先直接点击添加，页面如下

到 所有路由器地址 at 端口 68 位于本设备

打开路由器端口:

名字	协议	外部端口
新建进入规则	TCP+UDP	

→ 第一步

新建转发规则:

名字	源区域	目标区域
新建转发规则	lan	wan

Source NAT

点击添加后界面如下:

### 防火墙 - 通信规则 - (未命名规则)

本页面可以更改通信规则的高级设置。比如：需匹配的源主机和目标主机。

Rule is enabled  禁用

名字  **第二步，填上名字**

限制地址

协议

匹配CMP类型

源区域

- 任意区域
- ipsec: (55)
- lan: lan
- vpn: vpn **第三步，默认是wan区域，选为vpn区域**
- wan: wan

源MAC地址

源地址

源端口

目标区域

- 设备 (输入)
- 任意区域 (转发)
- ipsec: (55)
- lan: lan
- vpn: vpn
- wan: wan

**注意，目的区域需要根据需要填写**

目标地址

目标端口  **第四步，填上目的端口80**

动作

保存应用后，页面如下：

来自 所有主机 位于 wan  
到 所有路由地址 位于 本设备

Allow-ICMPv6-Forward	IPv6-ICMP 和 types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type 来自 所有主机 位于 wan 到 所有主机 位于 所有区域	Accept forward 并且限制到 1000 包 每 second	<input checked="" type="checkbox"/>	<input type="button" value="修改"/> <input type="button" value="删除"/>
SSH	任何 TCP 来自 所有主机 位于 wan 到 所有路由地址 于 端口 22 位于 本设备	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="修改"/> <input type="button" value="删除"/>
vpn80	任何 TCP, UDP 来自 所有主机 位于 vpn 到 所有路由地址 于 端口 80 位于 本设备	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="修改"/> <input type="button" value="删除"/>

打开路由链端口:

名字	协议	外部端口
<input type="text" value="新建进入规则"/>	<input type="text" value="TCP+UDP"/>	<input type="text" value=""/>

新建转发规则:

## 1.4.7.4.2 自定义通信规则

云设备的通信规则，可以根据需要配置对应的通信规则。如可以拒绝某些主机之间的通信，禁止某些主机走 vpn 区域。下面用两个例子简单说明。如禁止源 ip172.18.188.191 走 vpn 区域，操作如下：

名字  → 填写通信规则名字

限制地址

协议  → 必须选择对应协议，这里选any

匹配ICMP类型

源区域

- 任意区域
- ipsec: (空)
- lan: lan: → 选择源地址所在的区域
- vpn: vpn: →
- wan: wan: →

源MAC地址

源地址  → 填上需要禁止的源IP

源端口

目标区域

- 设备 (输入)
- 任意区域 (转发)
- ipsec: (空)
- lan: lan: →
- vpn: vpn: → 选择需要禁止的目标区域
- wan: wan: →

目标地址  → 默认所有，也可指定目标地址

目标端口

动作  → 动作有接受、拒绝，丢弃，这里选择丢弃

如禁止 172.18.188.0/24 与 172.18.100.0/24 之间通信。操作如下：

协议: 任何

匹配CMP类型: any

源区域:  任意区域  ipsec: (空)  lan: lan:  vpn: vpn:  wan: wan:

源MAC地址: 所有

源地址: 172.18.188.0/24 → 源地址可以写ip段

源端口: 所有

目标区域:  设备 (输入)  任意区域 (转发)  ipsec: (空)  lan: lan:  vpn: vpn:  wan: wan: → 由于目标段在wan区域, 故选择wan

目标地址: 172.18.100.0/24

目标端口: 所有

动作: 丢弃

注

意：源地址与目的地址都可以通过自定义方式填写指定 ip 或者 ip 段。以及源区域需要对应源地址，目标区域需要对应目标地址。指定源 mac 地址、端口可根据需要填写。

## 1.4.8 SNMP

云设备默认开启 SNMP，版本为 V2C。通过 SNMP 可以监控到云设备运行的状态，以及流量使用情况。页面如下：



默认

SNMP 端口为 161，Community 默认为 public，源地址默认是全部开放，可以根据需求，自行修改。

## 1.5 流量整形使用规则（EH 系列）

本文档主要分两方面介绍流量整形的使用规则，分别为【流量整形相关配置模块的说明】和【限速规则配置范例】。

### 1.5.1 流量整形

【流量整形-共享带宽】用于配置共享带宽规则，点击【新建共享带宽规则】进到修改界面，按需填写规则名，平均速率的上下行带宽以及最大速率的上下行带宽，速率

单位为 kbps。(注：新建共享带宽规则后，需要在【接口与共享带宽组】中绑定在对应接口)

【流量整形-每个 IP 地址】用于配置限制源 ip 的带宽值。点击【新建每 IP 带宽规则】进到修改界面，按需填写规则名，上下行带宽值，单位为 kbps。

界面如下：



The screenshot shows the Cloud Valley management interface. At the top, there is a navigation bar with the logo and menu items: 状态, 系统, 网络, 退出. Below the navigation bar, there are several tabs: 流量整形, 地址与域名, 接口与共享带宽组, 共享带宽规则, and Per IP 限速规则. The '流量整形' tab is selected and highlighted with a red box. Under this tab, there are two sub-sections: '流量整形 - 共享带宽' and '流量整形 - 每IP地址', both also highlighted with red boxes. The '流量整形 - 共享带宽' section contains a table with columns: 规则名, 平均速率, 最大速率, and 动作. The table lists five rules with their respective average and maximum rates and '删除' and '修改' buttons. Below the table is a '新建共享带宽规则' button. The '流量整形 - 每IP地址' section contains a table with columns: PerIP规则名, 上行, 下行, and 动作. The table lists two rules with their respective upload and download rates and '删除' and '修改' buttons. Below the table is a '新建每IP带宽规则' button.

规则名	平均速率	最大速率	动作
1m	下行 1024 kbps 上行 1024 kbps	下行 1024 kbps 上行 1024 kbps	删除 修改
50	下行 51280 kbps 上行 51280 kbps	下行 51280 kbps 上行 51280 kbps	删除 修改
30M	下行 1024 kbps 上行 1024 kbps	下行 30720 kbps 上行 30720 kbps	删除 修改
15M	下行 1024 kbps 上行 1024 kbps	下行 15360 kbps 上行 15360 kbps	删除 修改
5m	下行 1024 kbps 上行 1024 kbps	下行 5120 kbps 上行 5120 kbps	删除 修改

PerIP规则名	上行	下行	动作
10m	10240 kbps	10240 kbps	删除 修改
5M	5120 kbps	5120 kbps	删除 修改

## 1.5.2 地址与域名

用于配置要的限制的源地址以及目的地址，可以分别选择域名、子网以及 ip 段，多个域名填写格式为 abc.com/cba.com

ip 段填写格式为 172.18.100.1-172.18.100.10 子网填写格式为

172.18.188.0/24，单个 ip 填写格式为 172.18.100.10/32 多个子网填写

格式为 172.18.188.0/24,172.18.189.0/24 界面如下：



流量整形 | 地址与域名 | **接口与共享带宽组** | 共享带宽规则 | Per IP 限速规则

### 对象列表

	type	host	
youtube	域名 ▾	abc.com/cba.com	
ip	IP段 ▾	172.18.100.195	
test	子网 ▾	172.18.188.0/24	
facebook	域名 ▾	facebook.com	
ipsegment	IP段 ▾	172.18.100.1-172.18.100.1	

### 1.5.3 接口与共享带宽组

【接口-速率】用于限制接口的总速率，如 VPN 带宽为 10M，设置 vpn 接口上下行带宽为 10240kbps。

【共享带宽组】用于把【流量整形-共享带宽】中创建的带宽规则绑定在相应的接口上，界面如下

Cloud valley 状态 ▾ 系统 ▾ 网络 ▾ 退出 未保存

流量整形 | 地址与域名 | **接口与共享带宽组** | 共享带宽规则 | Per IP 限速规则

### 接口 - 速率

接口	启用	上行	下行	动作
vpn	启用	52720 kbps	52720 kbps	 
wan	启用	51200 kbps	309600 kbps	 



### 共享带宽组

vpn 

规则名	平均速率	最大速率
30M	下行 1024 kbps 上行 1024 kbps	下行 30720 kbps 上行 30720 kbps
15M	下行 1024 kbps 上行 1024 kbps	下行 15360 kbps 上行 15360 kbps
5m	下行 1024 kbps 上行 1024 kbps	下行 5120 kbps 上行 5120 kbps
1m	下行 1024 kbps 上行 1024 kbps	下行 5120 kbps 上行 5120 kbps

## 1.5.4 共享带宽规则

用于配置源主机到目的主机的共享带宽规则，可以指定接口以及协议。界面如下：



The screenshot shows the '共享带宽规则' (Shared Bandwidth Rules) configuration page. At the top, there is a navigation bar with 'Cloud valley' logo and menu items: '状态', '系统', '网络', and '退出'. A '未保存的配置: 3' (Unsaved configurations: 3) indicator is on the right. Below the navigation bar, there are tabs for '流量整形', '地址与域名', '接口与共享带宽组', '共享带宽规则' (highlighted with a red box), and 'Per IP 限速规则'. The main content area is titled '共享带宽规则' and contains a table with columns: '接口', '目标', '源主机', '目的主机', '协议', '端口', '注解', and '排序'. A single rule is visible with the following values: 'vpn' for interface, '5m' for target, '100' for source host, 'googlevideo' for destination host, 'ANY' for protocol, and empty fields for port and annotation. There are '添加' (Add) and '删除' (Delete) buttons for this rule. At the bottom right, there are '保存&应用' (Save & Apply), '保存' (Save), and '复位' (Reset) buttons.

## 1.5.7 Per IP 限速规则

【每 IP 地址限速】用于配置源主机的限速规则，可以指定相应接口

【白名单】用于开放对源主机的带宽限制，可选择相应接口，IP 段或子网。页面如下：



The screenshot shows the 'Per IP 限速规则' (Per IP Rate Limiting Rules) configuration page. At the top, there is a navigation bar with 'Cloud valley' logo and menu items: '状态', '系统', '网络', and '退出'. A '未保存的配置: 3' (Unsaved configurations: 3) indicator is on the right. Below the navigation bar, there are tabs for '流量整形', '地址与域名', '接口与共享带宽组', '共享带宽规则', and 'Per IP 限速规则' (highlighted). The main content area is titled '每IP地址限速' and contains two sections: '每IP地址限速' and '白名单'. The '每IP地址限速' section has a table with columns: '接口', '对象', '流量策略', and '排序'. A single rule is visible with the following values: 'vpn' for interface, '100' for object, and '5M' for flow strategy. There are '添加' (Add) and '删除' (Delete) buttons for this rule. The '白名单' section has a table with columns: '接口', '类型', and '对象'. A single rule is visible with the following values: 'vpn' for interface, 'IP段' for type, and '172.18.100.133' for object. There are '添加' (Add) and '删除' (Delete) buttons for this rule.

## 1.5.6 Per IP 限速规则配置范例

使用需求：限制每个源主机的国际带宽不超过 5M，配

置步骤如下：第一步，在【流量整形】中新建每 IP 限制

的带宽为 5M。



Cloud valley 状态 系统 网络 退出

流量整形 地址与域名 接口与共享带宽组 共享带宽规则 Per IP 限速规则

### 流量整形 - 共享带宽

规则名	平均速率	最大速率	动作
新建共享带宽规则			

### 流量整形 - 每IP地址

PerIP规则名	上行	下行	动作
5m	5120 kbps	5120 kbps	删除 修改
新建每IP带宽规则			

第二步，

在【地址与域名】，添加源地址，可填子网，IP 段以及单个 ip。



流量整形 地址与域名 接口与共享带宽组 共享带宽规则 Per IP 限速规则

### 对象列表

类型	对象	动作
100	子网 172.18.100.0/24	删除
192	IP段 172.18.100.1-17.18.100.10	删除
102	IP段 172.18.100.102	删除

添加

第三步，在【Per IP 限速规则】配置相应规则，指定 VPN 接口。



流量整形 地址与域名 接口与共享带宽组 共享带宽规则 Per IP 限速规则

### 每IP地址限速

接口	对象	流量策略	排序	动作
vpn	100	5m		删除

添加

## 1.5.8 共享带宽规则配置范例

使用需求：限制用户在带宽空闲时，保障访问 youtube 的速率为 1M 以上，10M 以下，在带宽跑满并且有多条共享带宽规则情况下，将按照每条共享带宽规则的平均速率的比例（如总带宽为 6M，分别设置两条共享带宽规则的平均速率为 3M、6M，在带宽跑满情况下，两条共享带宽规则将按 1：2 的比例保障带宽分别为 2M、4M），保障访问的速率。

配置步骤如下：

第一步，在【流量整形】新建共享带宽规则，平均速率为 1024kbps，最大速率为 10240kbps。



流量整形 地址与域名 接口与共享带宽组 共享带宽规则 Per IP 限速规则

### 流量整形 - 共享带宽

规则名	平均速率	最大速率	动作
10m	下行 1024 kbps 上行 1024 kbps	下行 10240 kbps 上行 10240 kbps	<span>删除</span> <span>修改</span>

新建共享带宽规则

第二步，在【地址与域名】，添加名称为 youtube，类型选择【域名】，【对象】填 youtube.com。



Cloud valley 状态 系统 网络 退出 未保存的配置

流量整形 地址与域名 接口与共享带宽组 共享带宽规则 Per IP 限速规则

### 对象列表

类型	对象	操作
youtube	域名 <input type="text" value="youtube.com"/>	<span>删除</span>
ip	IP段 <input type="text" value="8.8.8.8"/>	<span>删除</span>

添加

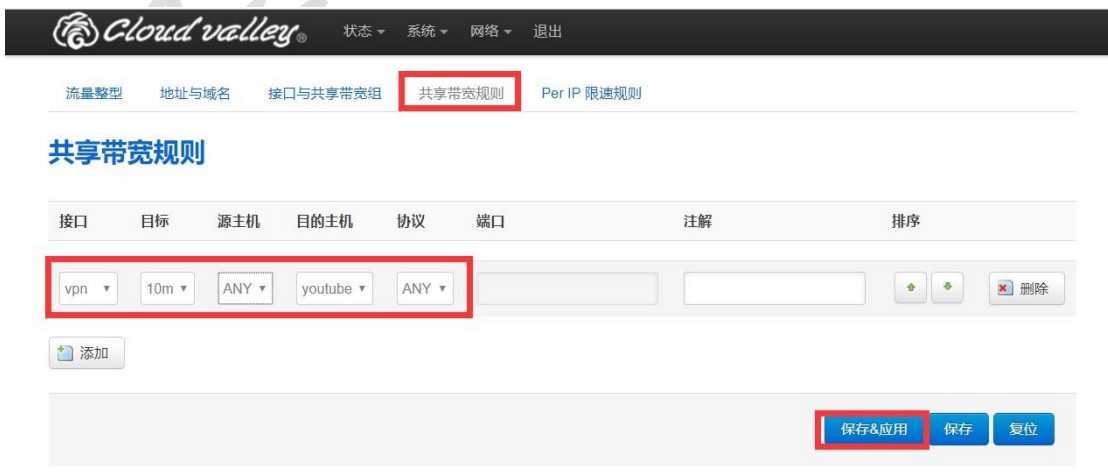
保存&应用 保存 复位

第三步，在【接口与共享带宽组】，把相应的共享带宽规则绑定在对应的接口，如绑定在 VPN 接口



The screenshot shows the '接口与共享带宽组' (Interface and Shared Bandwidth Group) configuration page. At the top, there are navigation tabs: '流量整形', '地址与域名', '接口与共享带宽组' (highlighted), '共享带宽规则', and 'Per IP 限速规则'. Below the tabs is a table titled '接口 - 速率' (Interface - Rate) with columns for '接口' (Interface), '启用' (Enabled), '上行' (Upload), '下行' (Download), and '动作' (Action). The table lists two interfaces: 'wan' and 'vpn'. Below the table is a '新增接口' (Add Interface) button. Underneath is the '共享带宽组' (Shared Bandwidth Group) section, with a 'wan' group and a 'vpn' group (highlighted). The 'vpn' group has a '修改' (Modify) button. Below the 'vpn' group is a table with columns for '规则名' (Rule Name), '平均速率' (Average Rate), and '最大速率' (Maximum Rate). The table lists a rule named '10m' with upload and download rates of 1024 kbps.

第四步，在【共享带宽规则】，根据需求选择对应的选项。



The screenshot shows the '共享带宽规则' (Shared Bandwidth Rule) configuration page. At the top, there are navigation tabs: '流量整形', '地址与域名', '接口与共享带宽组', '共享带宽规则' (highlighted), and 'Per IP 限速规则'. Below the tabs is a table with columns for '接口' (Interface), '目标' (Target), '源主机' (Source Host), '目的主机' (Destination Host), '协议' (Protocol), '端口' (Port), '注解' (Annotation), and '排序' (Sort). The table lists a rule with 'vpn' as the interface, '10m' as the target, 'ANY' as the source host, 'youtube' as the destination host, and 'ANY' as the protocol. Below the table is an '添加' (Add) button. At the bottom right, there are three buttons: '保存&应用' (Save & Apply, highlighted), '保存' (Save), and '复位' (Reset).

配置共享带宽规则分为两种情况。情况一：当 facebook 与 YouTube 需要共享 5M 带宽时，共享带宽规则的目标需要选定同一个带宽值，配置如下：



The screenshot shows the Cloud Valley management interface. The top navigation bar includes the logo and menu items: 状态, 系统, 网络, 退出. Below the navigation bar, there are tabs for 流量整形, 地址与域名, 接口与共享带宽组, 共享带宽规则, and Per IP 限速规则. The '共享带宽规则' tab is selected and highlighted with a red box. The main content area is titled '共享带宽规则' and displays a table with columns: 接口, 目标, 源主机, 目的主机, 协议, 端口, 注解, and 排序. Two rows are visible in the table, both with a '5M' target value highlighted by red boxes. The first row has 'youtube' as the destination host, and the second row has 'facebook' as the destination host. Each row also includes a '删除' (Delete) button.

接口	目标	源主机	目的主机	协议	端口	注解	排序
vpn	5M	ANY	youtube	ANY		2	+ - 删除
vpn	5M	ANY	facebook	ANY		3	+ - 删除

情

情况二：当 facebook 与 YouTube 分别需要 5M 带宽时，需要在【流量整形-共享带宽】中再新建一个 5M 的共享带宽，并绑定在【接口与共享带宽组】的共享带宽组，在【共享带宽规则】中的【目标】需要选定不同带宽值，配置如下：

Cloud valley 状态 系统 网络 退出

流量整形 地址与域名 接口与共享带宽组 共享带宽规则 Per IP 限速规则

### 流量整形 - 共享带宽


规则名	平均速率	最大速率	动作
5M	download 1024 kbps upload 1024 kbps	download 5120 kbps upload 5120 kbps	 删除  修改
facebook5M	download 1024 kbps upload 1024 kbps	download 5120 kbps upload 5120 kbps	 删除  修改

 新建共享带宽规则 → 第一步, 新建共享带宽facebook5M

Cloud valley 状态 系统 网络 退出

流量整形 地址与域名 接口与共享带宽组 共享带宽规则 Per IP 限速规则

### 接口 - 限速

接口	启用	上行速率	下行速率	动作
wan	启用	20480 kbps	20480 kbps	 修改  删除
vpn	启用	10240 kbps	10240 kbps	 修改  删除

 新增接口

### 共享带宽组

wan  修改

规则名	平均速率	最大速率
vpn 		
5M	download 1024 kbps upload 1024 kbps	download 5120 kbps upload 5120 kbps
facebook5M	download 1024 kbps upload 1024 kbps	download 5120 kbps upload 5120 kbps

第二步, 把共享带宽绑定在VPN口

### 共享带宽规则

接口	目标	源主机	目的主机	协议	端口	注解	排序
vpn	facebook5M	ANY	facebook	ANY		3	
vpn	5M	ANY	youtube	ANY		2	

添加

选择不同的共享带宽作为目标

套谷百科