



WEB

RG-AS2T

RGOS 10.4(3b16)p5

V1.0



RGOS 10.4 (3b16)p5

<http://www.ruijie.com.cn/>

<http://webchat.ruijie.com.cn>

<http://www.ruijie.com.cn/service.aspx>

7× 24

4008-111-000

<http://bbs.ruijie.com.cn/portal.php>

[service@ruijie.com.cn](mailto:service@ruijie.com.cn)



1)

[] []

{x|y|...}

[x|y|...]

//

2)

---

---

3)

v

# 1 WEB

## 1.1 WEB

WEB IE  
 WEB WEB WEB WEB  
 WEB WEB IE

## 1.2

### 1.2.1

WEB WEB WEB PC  
 IPAD  
 IE6.0 IE7.0 IE8.0 IE maxthon WEB  
 1024\*768 1280\*1024 1440\*960

### 1.2.2

WEB  
 WEB  
 IP

## 1.3 WEB

WEB WEB " WEB "

---

WEB Enable Enable

---

## 1.4 WEB

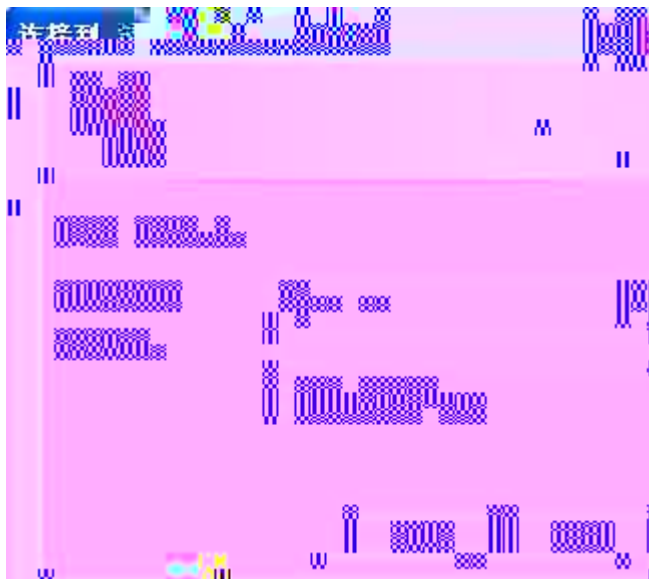
IP IP WEB  
 IP http://192.168.1.200,

1-1

交换机 WEB 管理平台



1-2



WEB

1-3 WEB



## 1.5

### 1.5.1 IP

" IP "

IP

1-4 IP



ip " "

1-5 IP



IP " "

## 1.5.2 VLAN

" VLAN "





交换机端口分为两种模式：

Access：该模式的端口只属于一个VLAN，只传输该VLAN的报文，一般用于与终端直连。

Trunk：该模式的端口可以属于多个VLAN，可传输多个VLAN的报文，一般用于与其它交换机互连。

注意：当端口模式为“Trunk”时将允许所有VLAN访问，指定的VLAN将成为Trunk口的Native VLAN。

端口	端口模式	VLAN ID
GigabitEthernet 0/1	access	1
GigabitEthernet 0/2	access	1
GigabitEthernet 0/3	access	1
GigabitEthernet 0/4	access	1
GigabitEthernet 0/5	access	1
GigabitEthernet 0/6	access	1
GigabitEthernet 0/7	access	1
GigabitEthernet 0/8	access	1
GigabitEthernet 0/9	access	1
GigabitEthernet 0/10	access	1
GigabitEthernet 0/11	access	1

保存

VLAN ID " "

### 1.5.3

" "

1-10

## 网关设置

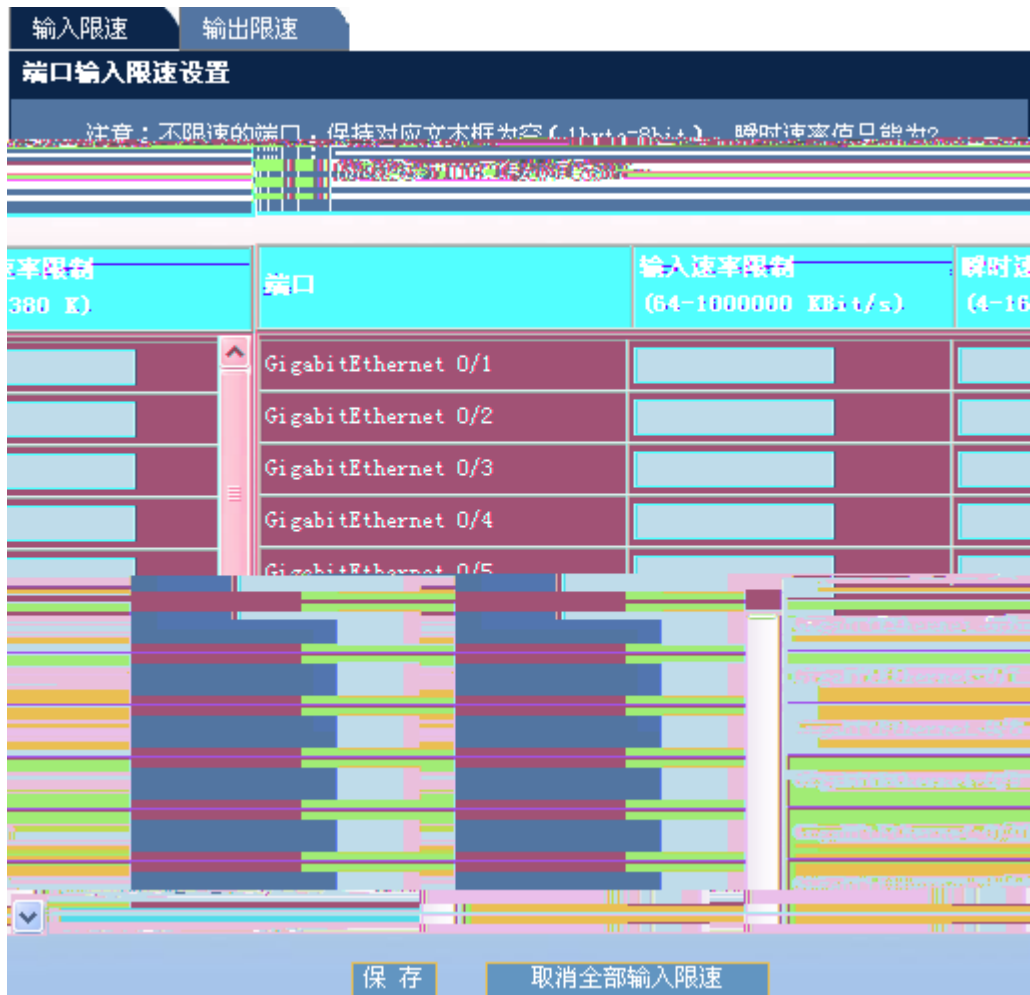
说明：网关相当于一个网络连接到另一个网络的“关口”，交换机无法转发的数据包就交给网关处理以便能完成数据包的转发过程。如果网关配置错误，可能导致设备与设备的连接中断。



网关IP地址：







2 n " "

1-15

输入限速

输出限速

## 端口输出限速设置

注意：不限速的端口，保持对应文本框为空（1byte=8bit）。瞬时速率值只能为2的n次方，10G口最小值为8。

端口	输出速率限制 (64-1000000 KBit/s)	瞬时速率限制 (4-16380 K)
GigabitEthernet 0/1	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/2	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/3	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/4	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/5	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/6	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/7	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/8	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/9	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/10	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/11	<input type="text"/>	<input type="text"/>

取消全部输出限速

## 1.5.7

**聚合端口设置**

注意：若选择的算法为缺省算法，配置后将不显示。

流量平衡算法选择：

<input type="checkbox"/>	聚合端口	最多成员端口数	二层端口	模式	成员端口

新建 全选 删除

1-17



**端口设置**

注意：若选择的参数该端口不支持，对应的参数设置将不生效！

端口：

状态： 双工： 速率： 流控：

描述：

端口	状态	双工	速率 (M)	流控	描述
Gi0/1	Down	Half	10	On	-
Gi0/2	Down	Half	10	On	-
Gi0/3	Down	Half	10	On	-
Gi0/4	Down	Half	10	On	-
Gi0/5	Down	Half	10	On	-
Gi0/6	Down	Half	10	On	-
Gi0/7	Down	Half	10	On	-
Gi0/8	Down	Half	10	On	-
Gi0/9	Down	Half	10	On	-
Gi0/10	Down	Half	10	On	-
Gi0/11	Up	Full	100	Off	-
Gi0/12	Down	auto	auto	Off	-

## 1.5.9

**DHCP 中继设置**

说明：DHCP中继可以实现不同子网之间的IP分配，相当于一个中转站，它将收到的客户端请求报文转发给指定的DHCP服务器，并将收到的服务器响应报文转发给DHCP客户端。

开启DHCP中继  
 关闭DHCP中继

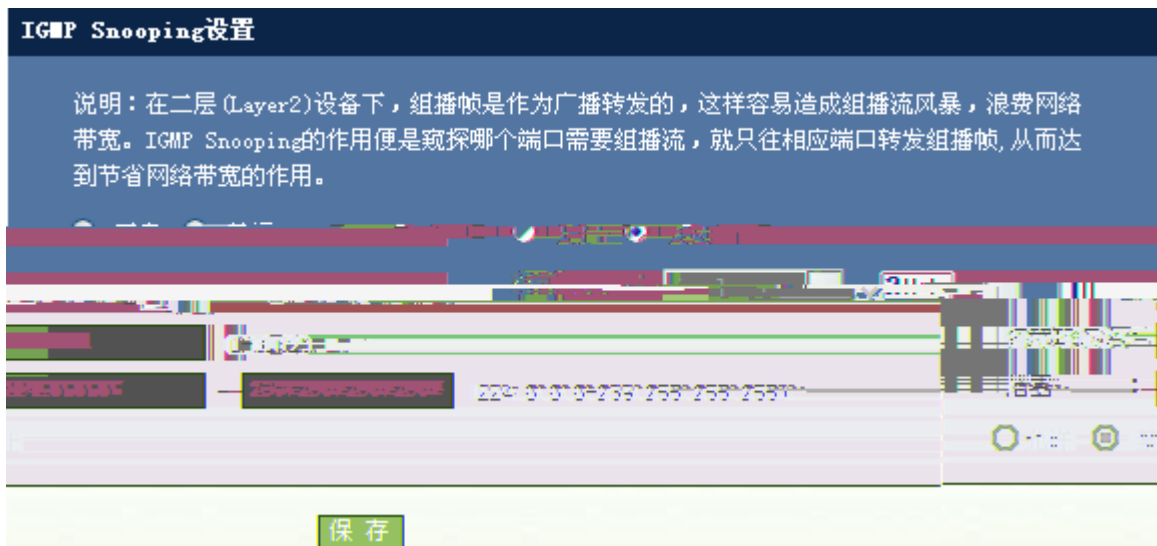
**DHCP服务器**

DHCP服务器：

**DHCP服务器**

/	DHCP		
/	DHCP	" "	" "
	DHCP		
	DHCP	" "	DHCP
		" "	

### 1.5.10 IGMP Snooping



IGMP Snooping " " ivgl  
 svgl ivgl-svgl svgl ivgl-svgl IP " "  
 IGMP Snooping " " " "

### 1.5.11 STP

" STP "

STP

1-21 STP

### STP设置

说明：STP通过有选择性地阻塞网络中的多余链路，保证网络中无环路产生；若网络出现故障导致链路失效，又能提供相应的链路备份，保证网络稳定运行。

开启STP功能： (默认开启的是MSTP)

MSTP基本设置：

MST名称：

MST修改值： (0-65535)

实例值： (1-64)

VLAN范围： (如输入100或100-200或100-200/250/300-2000)

端口设置：

端口：

设为快速端口  开启BPDU过滤

### MST 实例-VLAN 对应表：

实例	VLAN
(Table content is mostly blank in the image)	

" STP " " "

STP MSTP MSTP  
BPDU " "

MSTP MSTP VLAN -VLAN " "

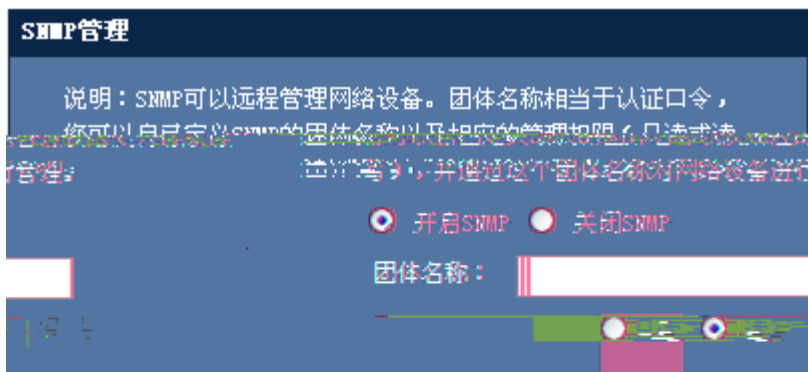
-VLAN

## 1.5.12 SNMP

" SNMP "

SNMP

1-22 SNMP



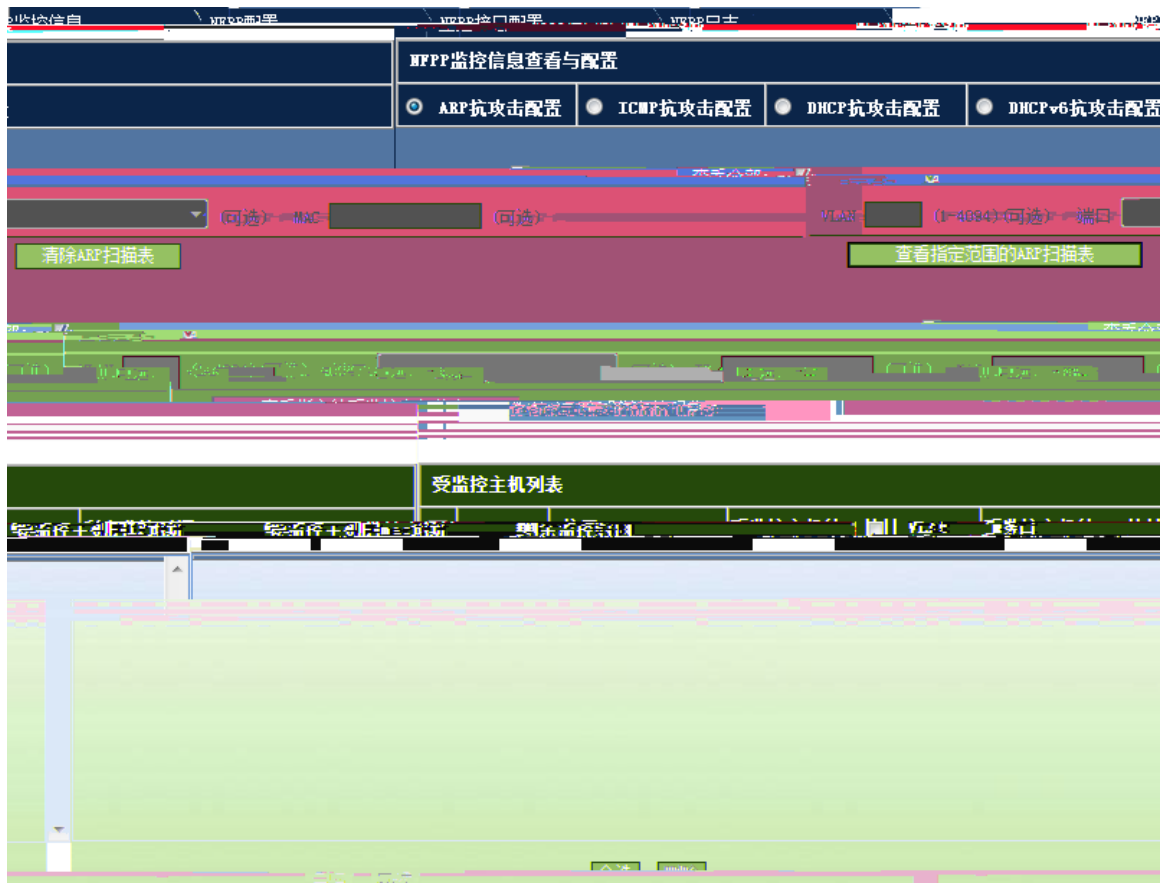
SNMP " SNMP" " SNMP" " "

### 1.5.13 NFPP

" NFPP "

NFPP

1-23 NFPP



## NFPP

### 1) ARP

1-24 NFPP —ARP

EFPP 监控信息查看与配置

查看全部:

(可选) MAC  (可选) VLAN  (1-4094) (可选) 端口

查看指定范围的ARP扫描表 清除ARP扫描表

查看全部:  查看

(1-4094) (可选) 端口  (可选) IP  (可选) MAC  (可选) VLAN

查看指定的受监控主机信息

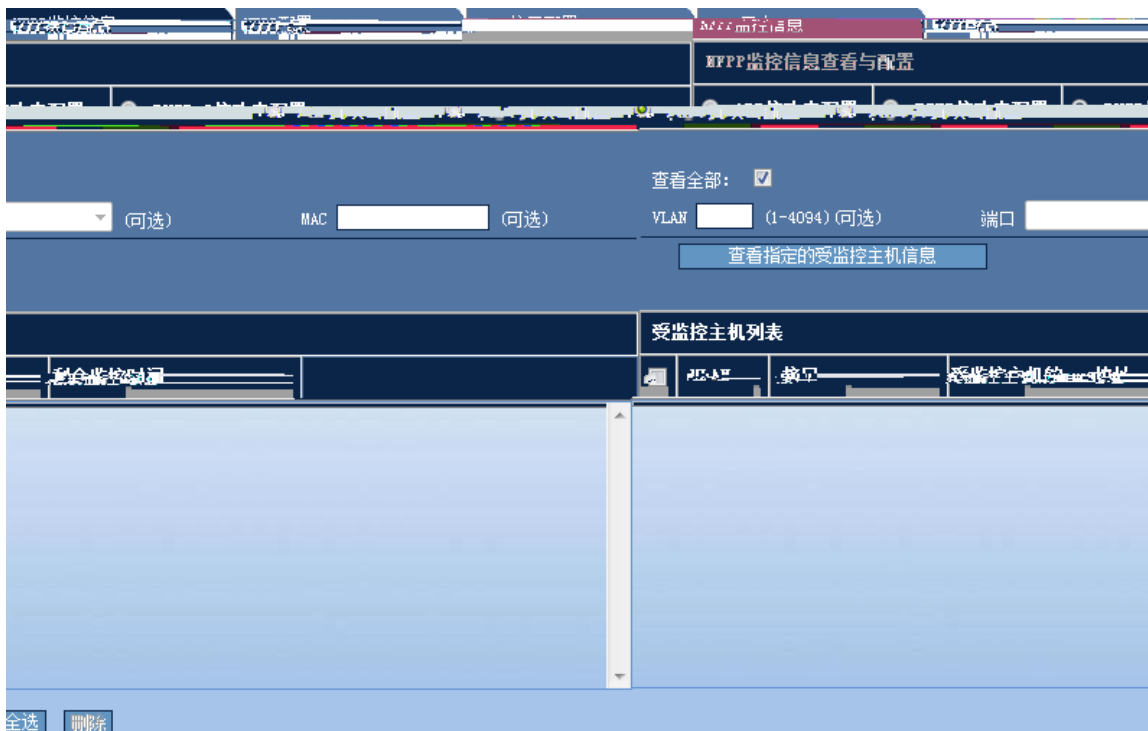
扫描表信息

N	interface	IP address	MAC address	timestamp	VLAN
	Fa0/40	-	001a.a942.f27f	2016-6-6 11:8:53	1
	Fa0/40	-	001a.a942.f27f	2016-6-6 11:11:2	1
		001a.a942.f27f	2016-6-6 11:12:2	Fa0/40	-
		001a.a942.f27f	2016-6-6 11:13:3	Fa0/40	-
		001a.a942.f27f	2016-6-6 11:14:4	Fa0/40	-
		001a.a942.f27f	2016-6-6 11:15:4	Fa0/40	-
		001a.a942.f27f	2016-6-6 11:16:5	Fa0/40	-
		001a.a942.f27f	2016-6-6 11:17:13	Fa0/40	-
		001a.a942.f27f	2016-6-6 11:18:14	Fa0/40	-
		001a.a942.f27f	2016-6-6 11:19:15	Fa0/40	-
		001a.a942.f27f	2016-6-6 11:20:23	Fa0/40	-
		001a.a942.f27f	2016-6-6 11:21:24	Fa0/40	-
		001a.a942.f27f	2016-6-6 11:22:24	Fa0/40	-
		001a.a942.f27f	2016-6-6 11:23:25	Fa0/40	-
		001a.a942.f27f	2016-6-6 11:24:26	Fa0/40	-
		001a.a942.f27f	2016-6-6 11:25:34	Fa0/40	-

ARP

ARP

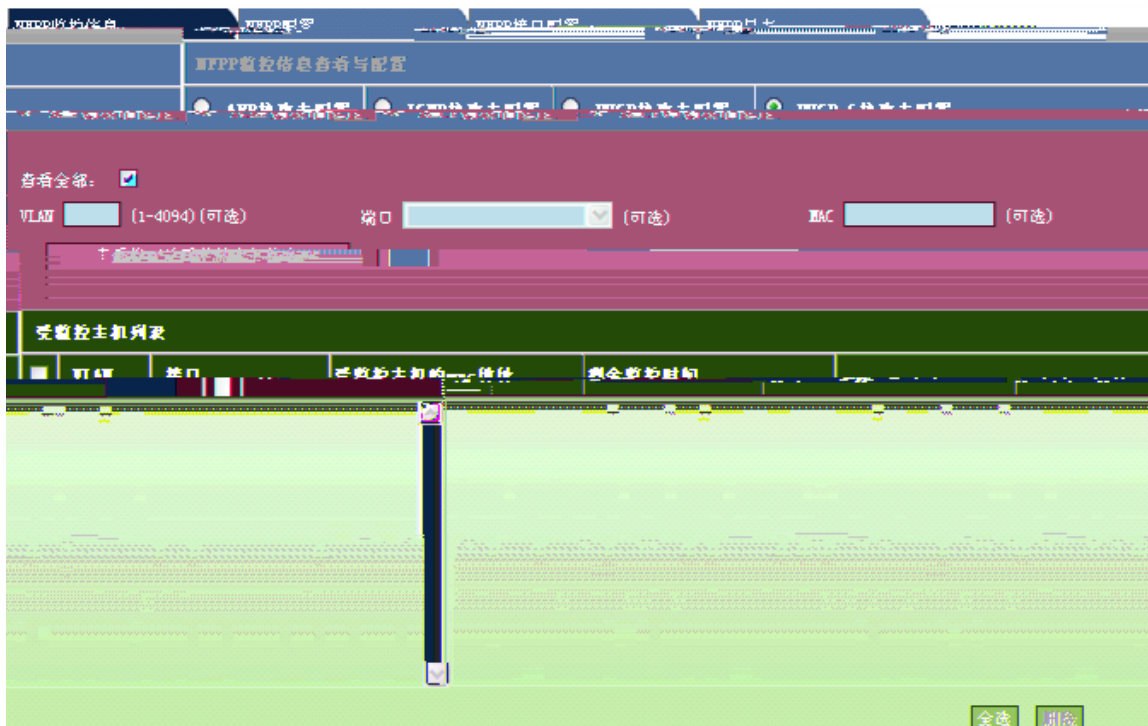




DHCP

4) DHCPv6

1-27 NFPP —DHCPv6

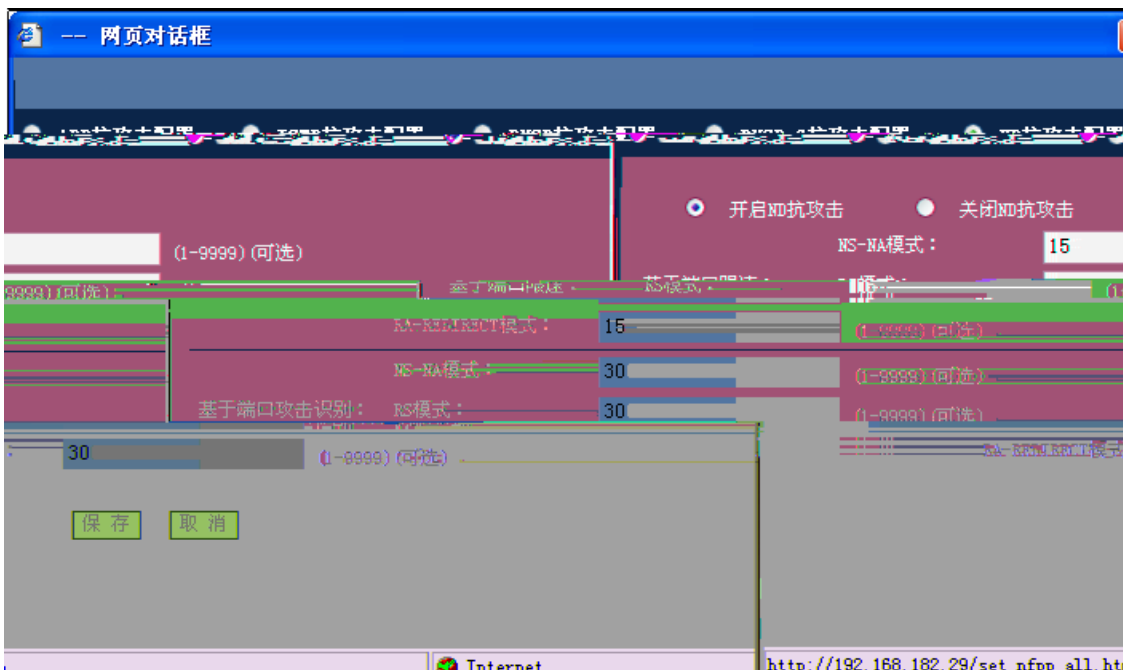




CPU

2) NFPP

1-30 NFPP



NFPP

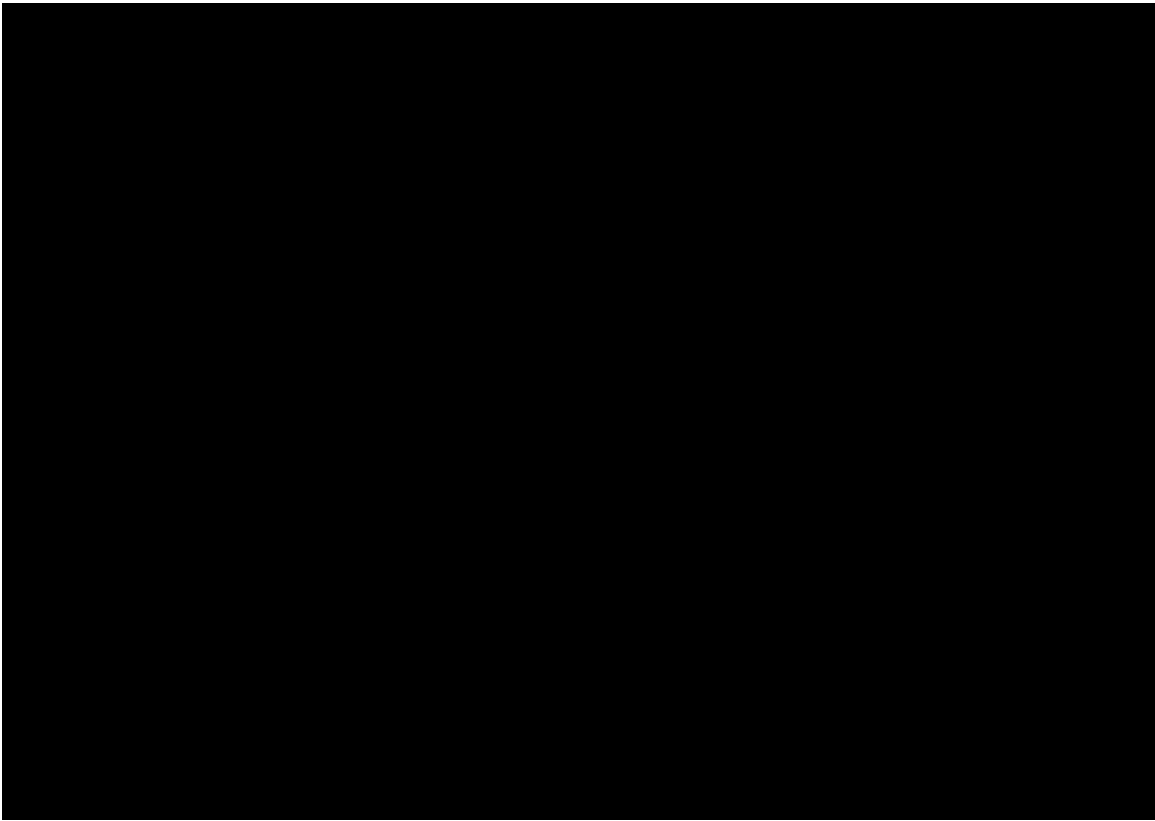
NFPP

NFPP

NFPP

1) ARP

1-31 NFPP —NFPP ARP



ARP            NFPP

"        "

2) ICMP

1-32 NFPP        —NFPP        ICMP





DHCP

NFPP

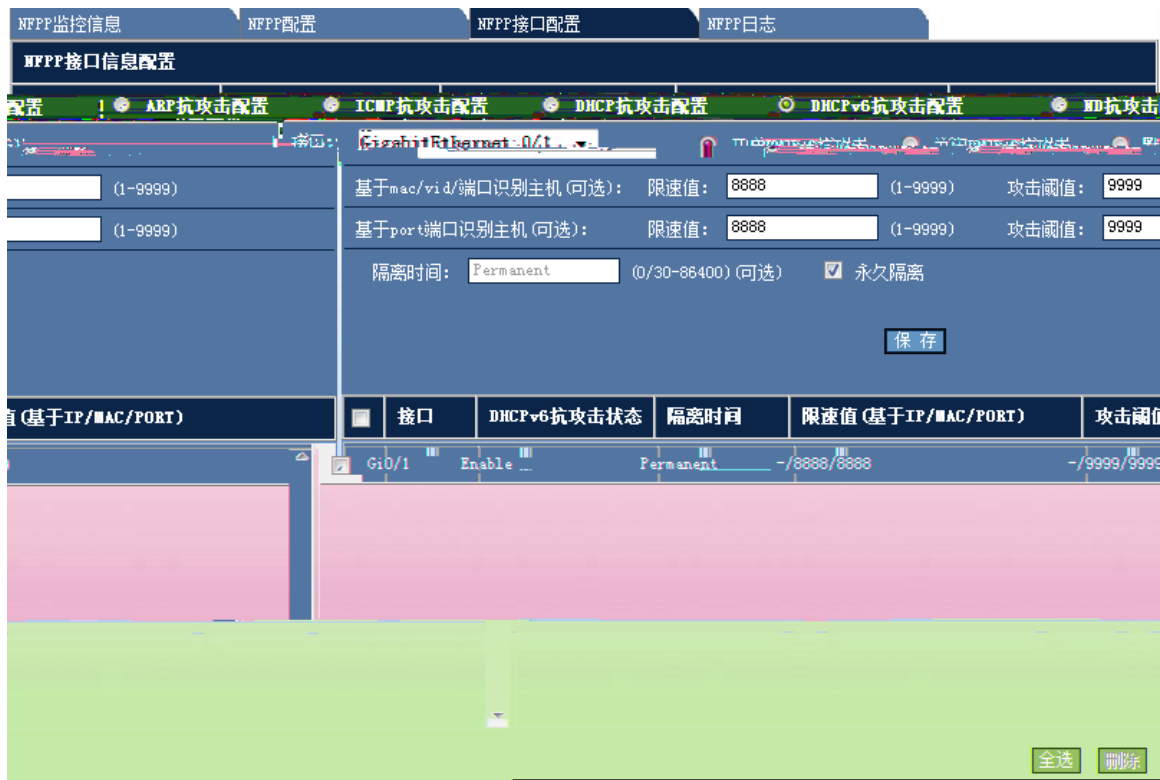
" "

4) DHCPv6

1-34 NFPP

—NFPP

DHCPv6



DHCPv6

NFPF

" "

5) ND

1-35 NFPF

—NFPF

ND



ND

NFPP

" "

## NFPP

1-36 NFPP

配置

指定需要记录日志的VLAN ID (用“,”隔开，相连的区间可用“-”连接): 1-4094 (1-4094) (可选)

指定需要记录日志的端口 (可选)

GigabitEthernet 0/1 添加

GigabitEthernet 0/2 删除

GigabitEthernet 0/3 删除

保存 恢复默认值 查看日志缓冲区 清空日志缓冲区

速率 (长度)	需要记录日志的VLAN	需要记录日志的端口	缓冲区大小	生成系统消息 G消息数/时间
0	1-4094	Gi0/1, Gi0/2, Gi0/3,	1000	1024/8640

NFPP

" "

" "

" "

1-37

**MFPP日志信息配置**

日志缓冲区大小:  (0-1024) (可选) 生成系统消息速率: 消息数:  (0-1024) (可选) 时间长度:  (0-86400) (可选)

用(连接):  (1-4094) (可选) 指定需要记录日志的IP地址(用), (例外: 相应的区域可)

ernet 0/1  指定需要记录日志的端口(可选):

ernet 0/2

ernet 0/3

日志缓冲区:

Protocol	VLAN	Interface	IP address	MAC address	Reason	Timestamp

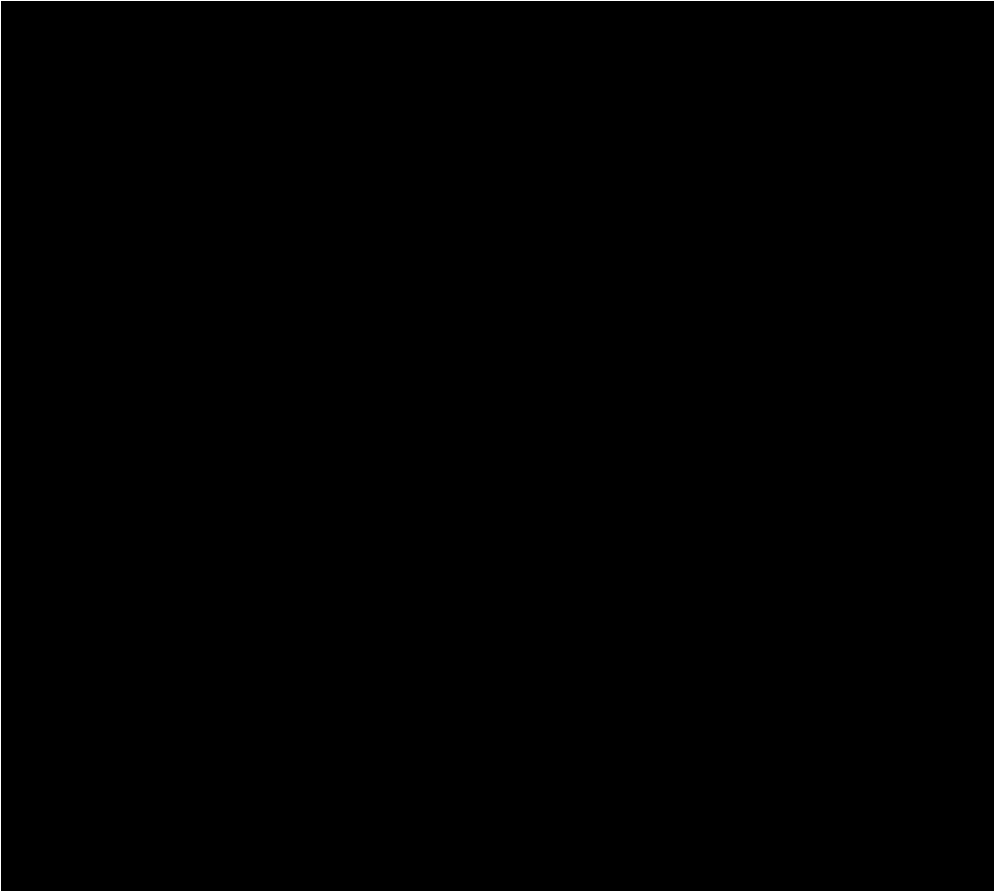
## 1.6

### 1.6.1 ARP

" ARP "

ARP

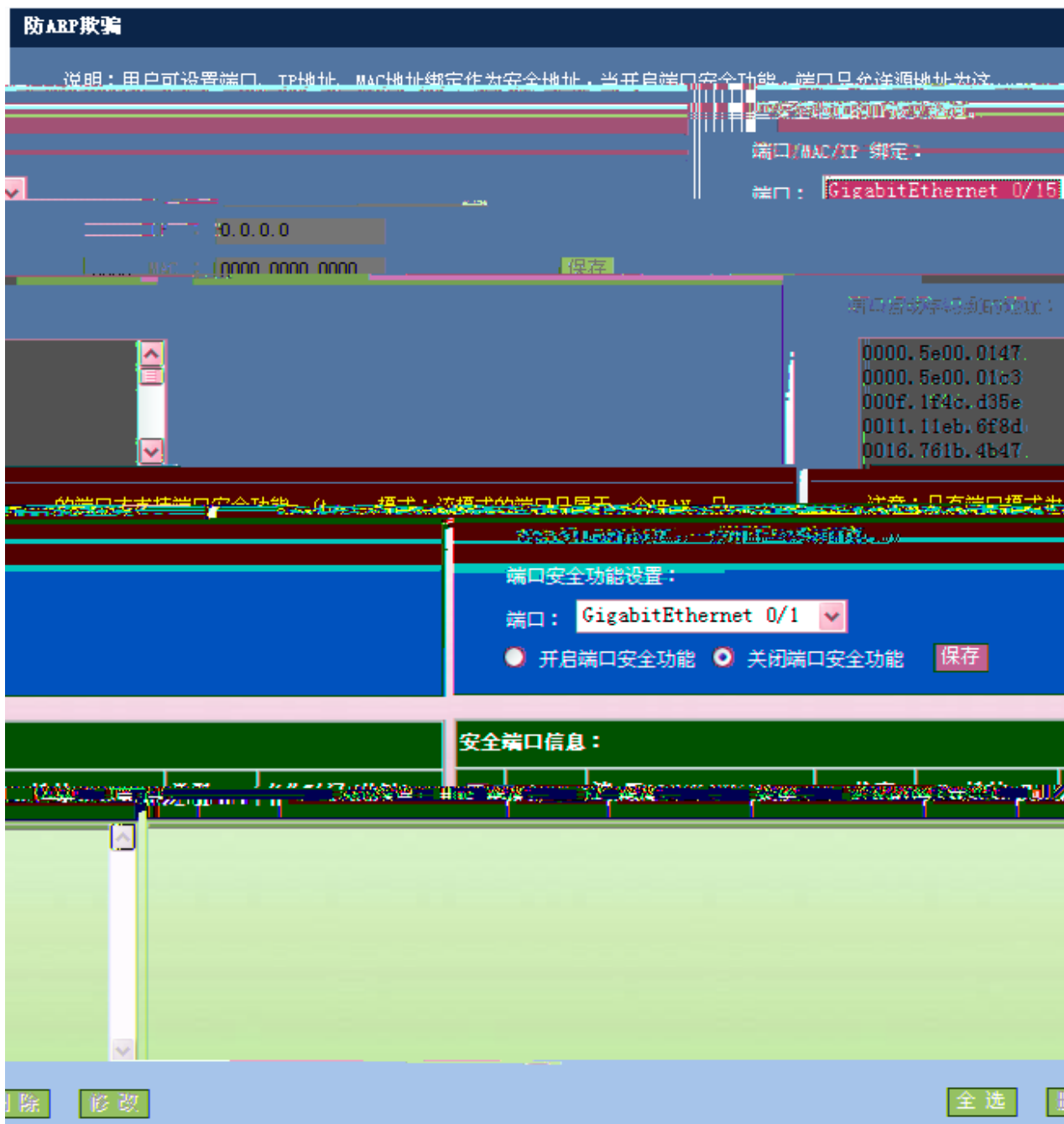
1-38 ARP



" "

" "

## 1.6.2 ARP



/MAC/IP

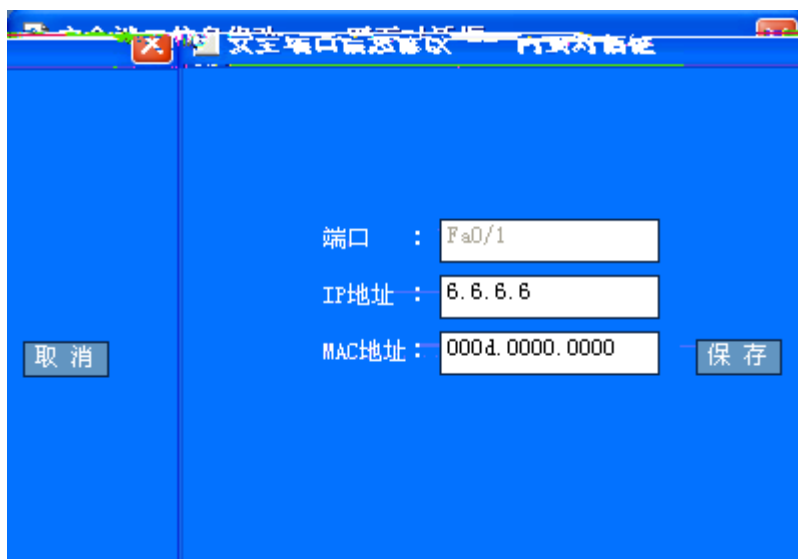
/MAC/IP  
MAC

IP MAC " "

GigabitEthernet 0/15

MAC

1-40





显示ACL信息    ACL配置    将ACL应用于端口

### ACL配置

通过，达到对网络接口数据的过滤。

IP标准访问控制列表：根据数据流的源IP地址制定匹配条件。（编号为1 - 99，1300 - 1999）

IP扩展访问控制列表：根据数据流的源IP地址、源端口、目的IP地址、目的端口制定匹配条件。

通配符掩码：通配符掩码规定了当一个IP地址与其他的IP地址进行比较时，该IP地址中哪些位应该被忽略；通配符掩码中的“1”表示忽略IP地址中相应的位，而“0”则表示该位必须保留。如果忽略了通配符掩码，0.0.0.0将被认为是缺省的屏蔽字。

配置标准IP访问列表     配置扩展IP访问列表

规则：

列表 ID (名称):  (1-99><1300-1999>)

IP地址： 任意源IP地址

指定IP地址范围： 通配符掩码： (可选)

显示ACL信息

ACL配置

将ACL应用于端口

## ACL配置

说明：ACL即访问控制列表（Access Control Lists），通过配置一系列匹配规则，对指定数据流（如限定的源IP地址、端口号等）执行允许或禁止通过，达到对网络接口数据的过滤。

IP标准访问控制列表：根据数据流的源IP地址制定匹配条件。（编号为1-99、1300-1999）

IP扩展访问控制列表：根据数据流的源IP地址、源端口、目的IP地址、目的端口制定匹配条件

配置扩展IP访问控制列表

配置扩展IP访问控制列表时，源IP地址、源端口、目的IP地址、目的端口和通配符掩码都必须指定。如果省略了通配符掩码，0.0.0.0将被认为是设备的环回地址。通配符掩码和IP地址的每一位对应一位，而“0”则表示该位

配置扩展IP访问列表

配置标准IP访问列表

规则：

列表 ID (名称):

协议：

源IP地址:

任意源IP地址:

指定IP地址范围:

通配符掩码:

(可选)

目的IP地址:  任意目的IP地址

指定IP地址范围:

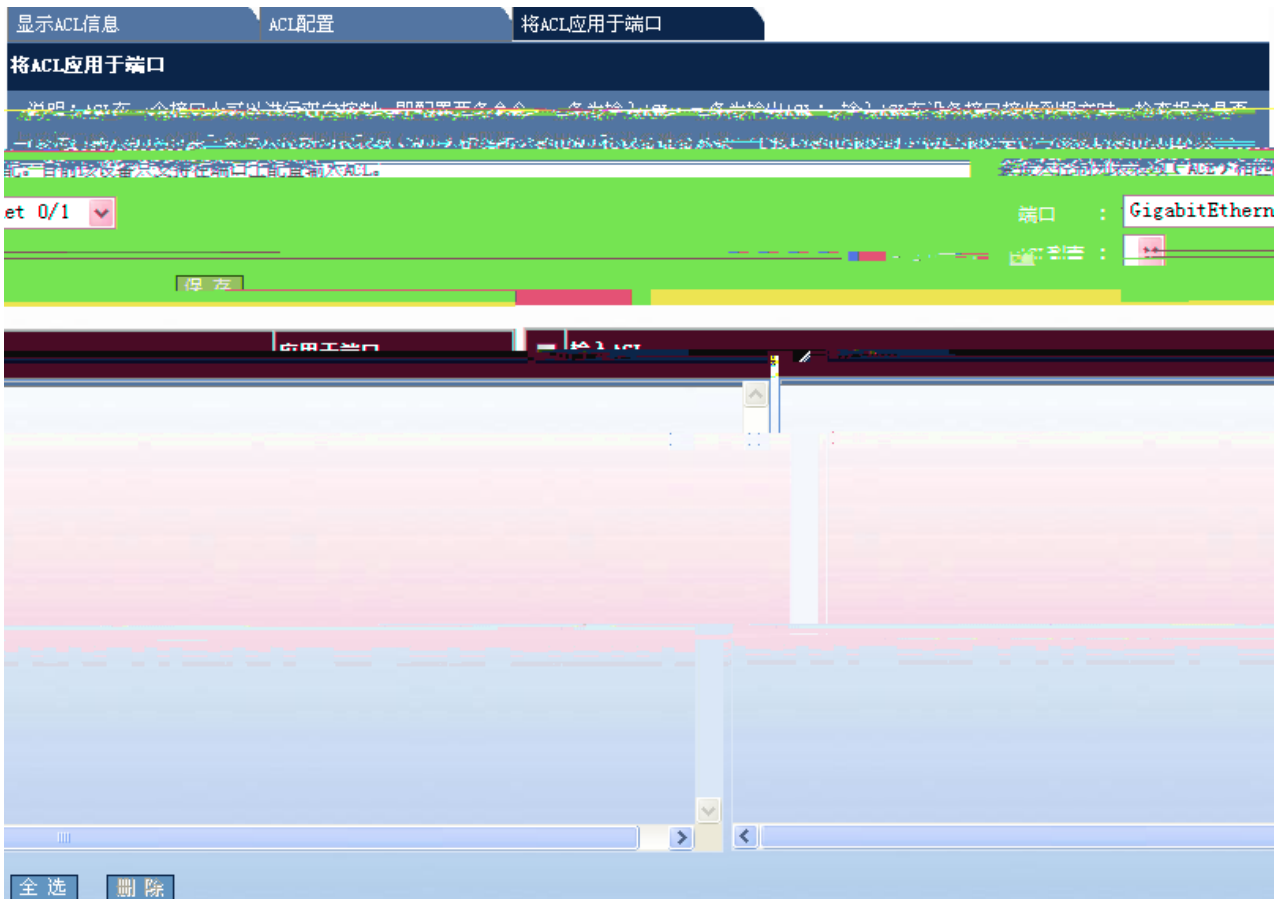
通配符掩码:  (可选)

目的端口:  (1-65535) (可选)

保存

ID

TCP



ACL

ACL

" "

" "

PC

ACL

PC

WEB

### 1.6.5 IP Source Guard

#### IP Source Guard

IP Source Guard                      IP                      [VLAN   MAC   IP   PORT]

IP Source Guard                      DHCP Snooping                      DHCP Snooping                      IP  
     IP Source Guard                      DHCP                      IP  
     IP

IP Source Guard      DHCP Snooping      DHCP Snooping

" IP Source Guard"

IP Source Guard

1-46 IP Source Guard



IP Source Guard

IP+MAC

"

IP+MAC

( )"

IP





### 1.6.7 GSN

" GSN"

GSN

1-49 GSN



GSN

GSN

GSN

GSN

GSN

SMP server

SMP server

v1

v2 v3

Community User

" "

GSN

GSN

" "

" "

### 1.6.8 CPP

" CPP "

CPP

## arp报文接收统计信息

Slot	Type	Pps	Total	Drop
MainBoard	arp	10	324430	0

1-52

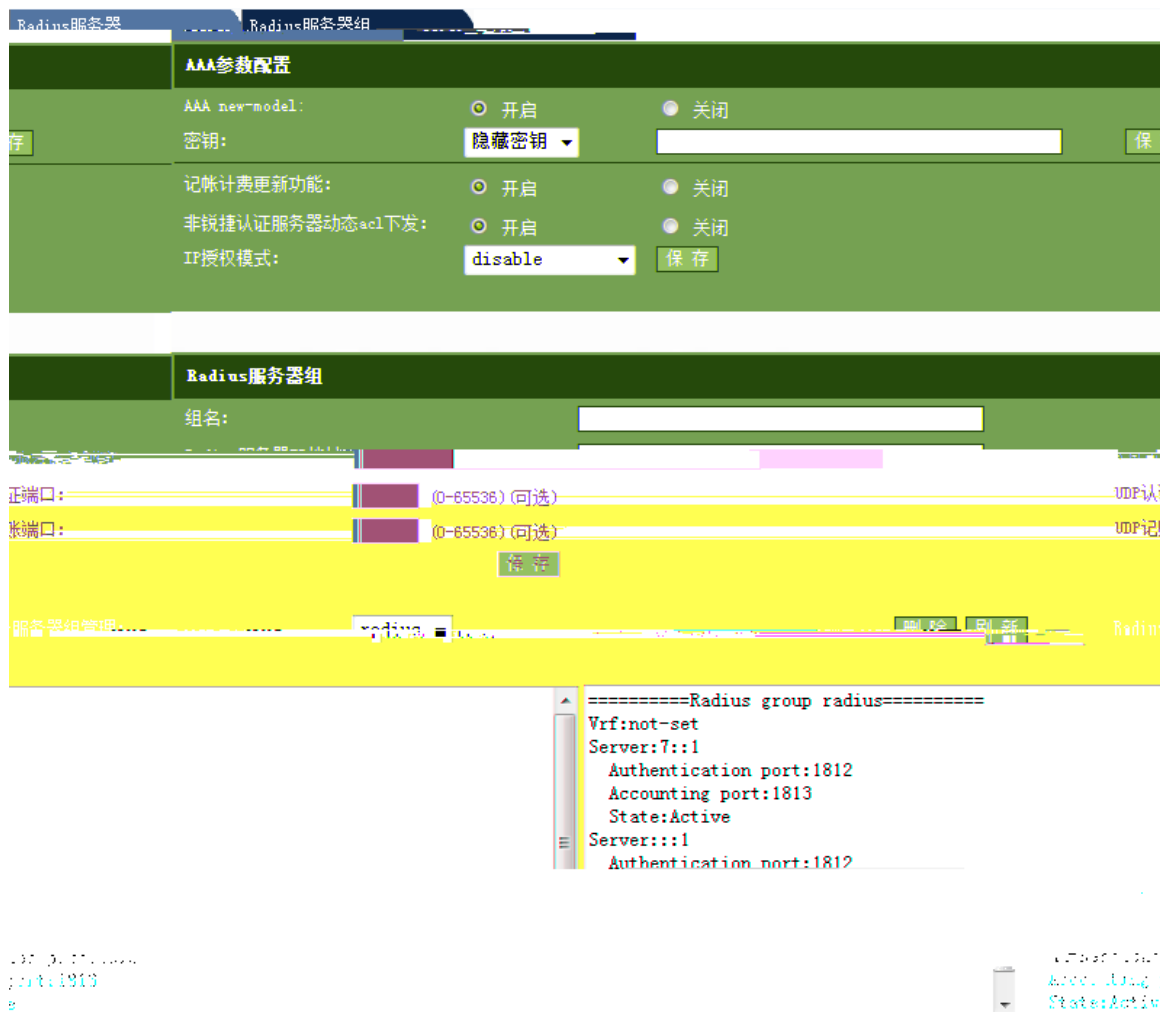
## 各类型报文的带宽和优先级配置状态

Type	Pps	Pri
tp-guard	180	7
arp	180	5
dot1x	2000	4
rldp	180	7
rerp	180	7
erps	180	7
bpdu	180	6
tunnel-bpdu	180	6
ipv4-icmp-local	1600	6
lldp	180	5
lldp_cdp	180	5
cfm-pdu	180	5

1-53







RADIUS IP

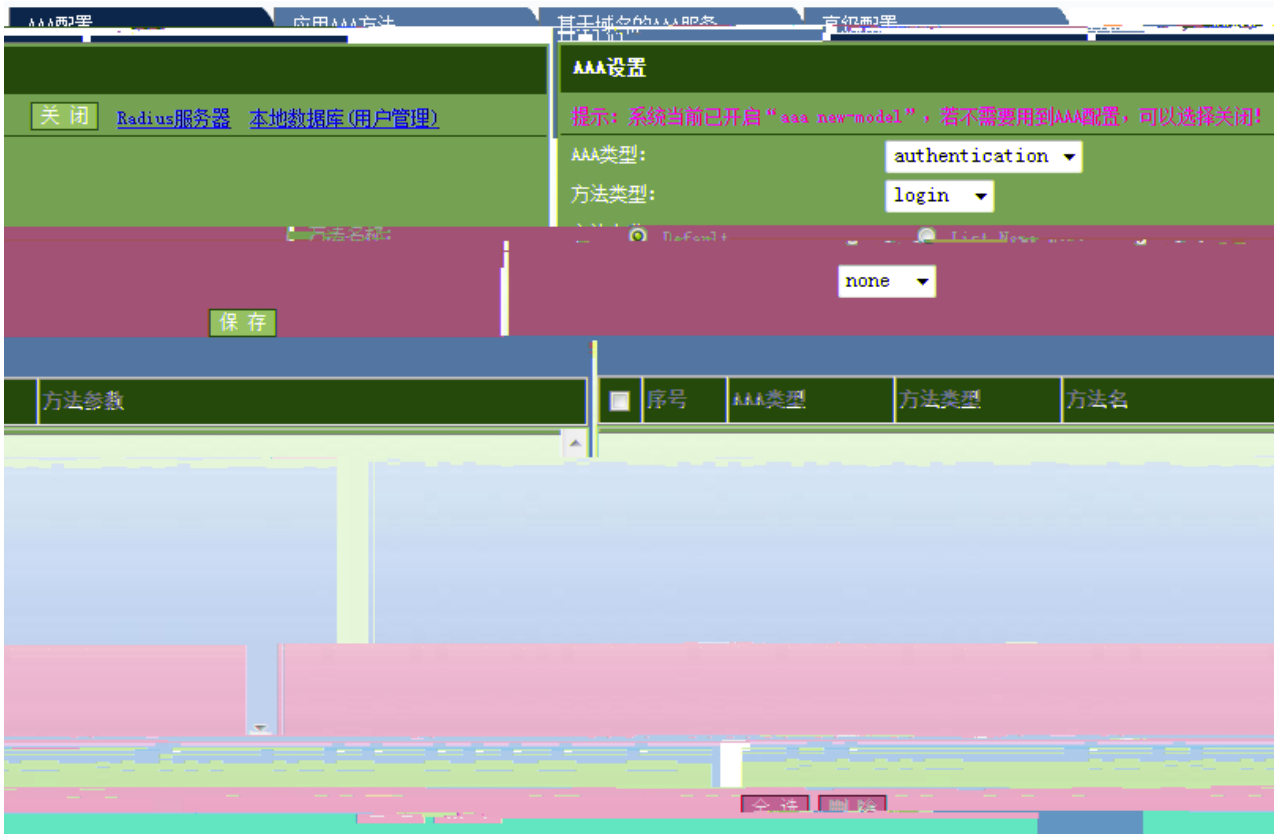
Radius

### 1.6.10 AAA

" AAA "

AAA

1-56 AAA



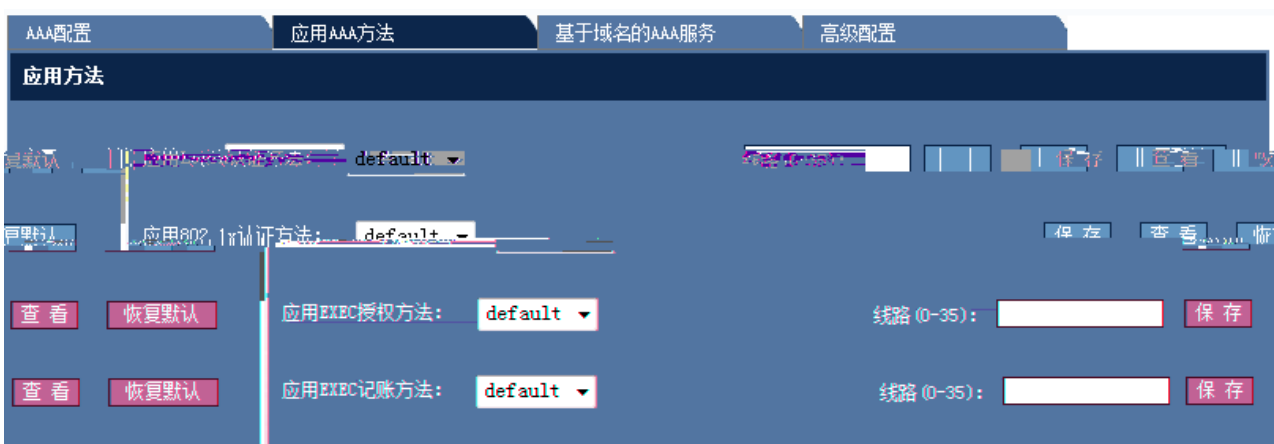
## AAA

```

AAA authentication authorization accounting AAA login enable
ppp dot1x exec command network List Name
local group " "
    
```

## AAA

1-57 AAA





AAA配置    应用AAA方法    基于域名的AAA服务    高级配置

**监视AAA用户**

当前AAA用户:  刷新

---

**配置支持VRF的AAA组**

RADIUS服务器组名:     VRF名:     保存

**用户认证失败锁定**

保存    login登录用户尝试失败次数 (1-2147483647):   
失败被锁定的时间 (1-2147483647):

刷新    清除    当前配置中的用户列表:

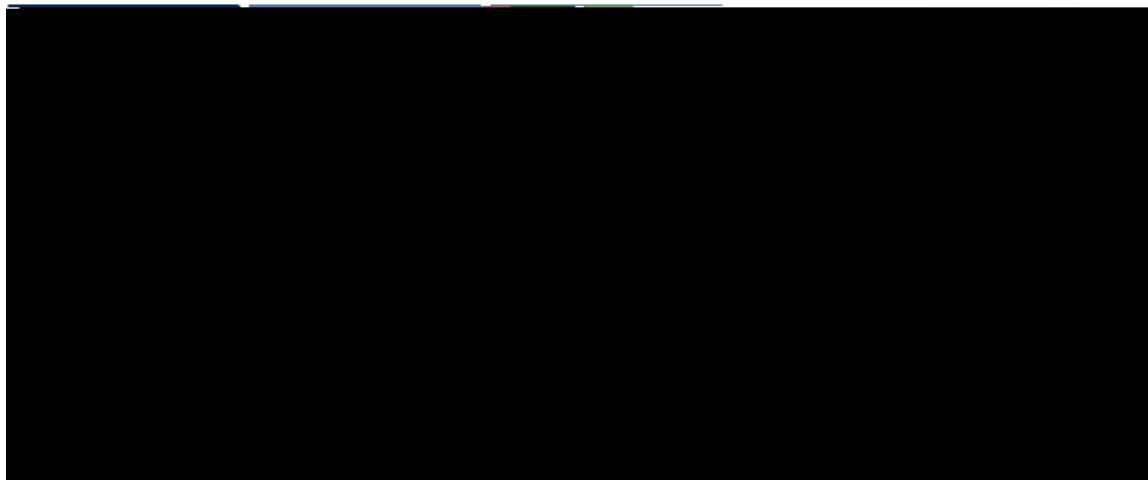
Name	Tries	Lock	Timeout (min)
AAA	AAA	VRF	AAA

### 1.6.11 Dot1x

" Dot1x "

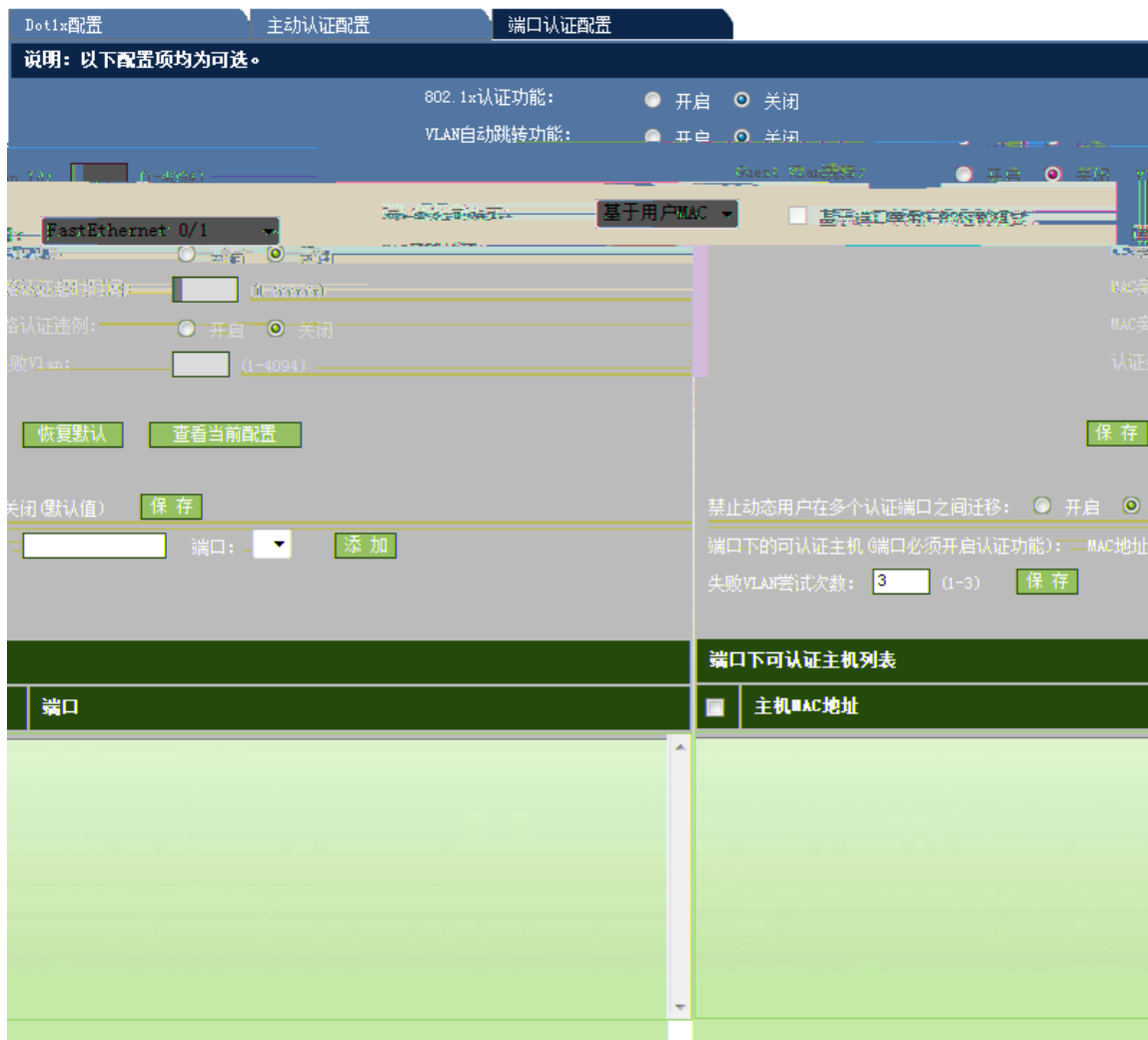
Dot1x

1-60 Dot1x



Dot1x

Dot1x



Dot1x

" "

" "

1-63            2

禁止动态用户在多个认证端口之间迁移： 开启  关闭(默认值)

端口下的可认证主机(端口必须开启认证功能)：MAC地址： 端口：

失败VLAN尝试次数： (1-3)

**端口下可认证主机列表**

主机MAC地址	端口
0011.1111.2323	FastEthernet 0/1

VLAN " " 802.1x " " MAC

### 1.6.12

1-64

### 智能绑定

手动查找IP MAC对应信息       通过ARP表查看IP MAC对应信息

IP地址:      

MAC地址:      

<input type="checkbox"/>	序号	IP	MAC
[Content obscured by redaction]			

IP	MAC				
	IP	MAC	MAC	"	"
ARP	IP	MAC		"	"
1-65	ARP				

**智能绑定**

手动查找IP-MAC对应信息
  通过ARP表查看IP-MAC对应信息

序号	IP	MAC	Vlan	操作
1	192.168.23.14	bc30.5bbe.8f4f	1	绑定
2	192.168.23.39	0025.64c5.af05	1	绑定
3	192.168.23.55	001...	1	绑定
4	192.168.23.70	001...	1	绑定
5	192.168.23.76	001...	5	绑定
6	192.168.23.81	001...	1	绑定
7	192.168.23.84	001...	1	绑定

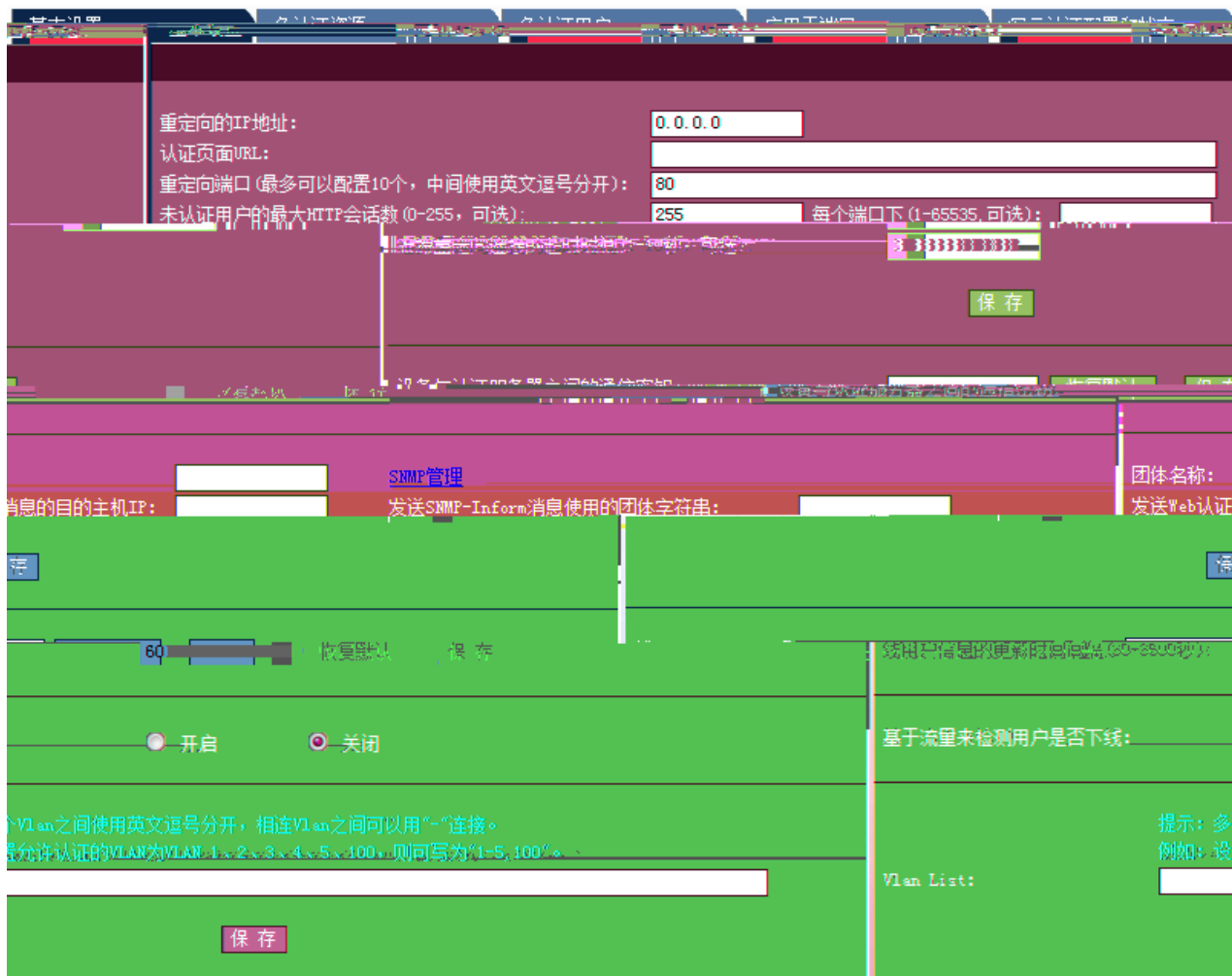
刷新

### 1.6.13 WEB

" web "

web

1-66 web



web IP URL HTTP (0-255 )  
 Web IP  
 SNMP-Inform , ,  
 80 Vlan List

基本设置 免认证资源 免认证用户 应用于端口 显示认证配置和状态

免认证资源(最大允许配置50个)

如果设置了port选项,则将用户IP与接入设备的端口进行绑定。如果接入/汇聚设备启用了ARP CHECK功能,那么需要对免认证的用户IP范围进行ARP绑定,需要配置arp关键字。

IP:  子网掩码(可选):  ARP

序号	IP地址	子网掩码	ARP绑定
1	1.2.3.6	255.255.255.0	Off

IP

1-68

基本设置 免认证资源 免认证用户 应用于端口 显示认证配置和状态

免认证用户(最大允许配置50个)

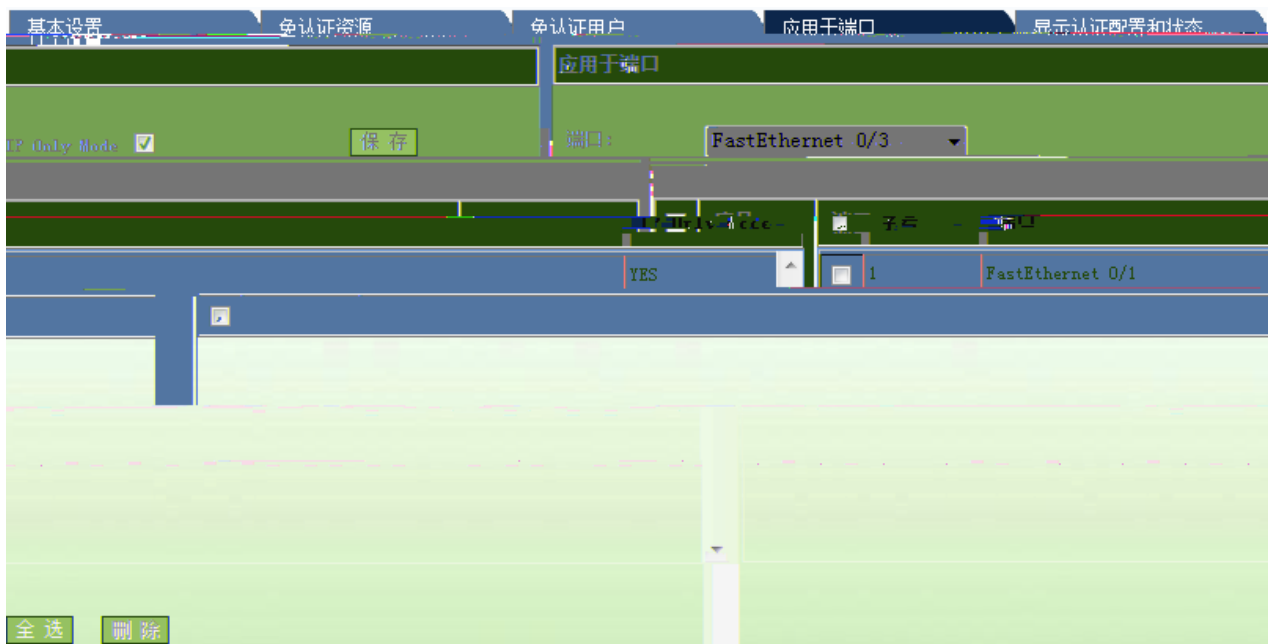
如果设置了port选项,则将用户IP与接入设备的端口进行绑定。如果接入/汇聚设备启用了ARP CHECK功能,那么需要对免认证的用户IP范围进行ARP绑定,需要配置arp关键字。

IP:  子网掩码(可选):  端口:  ARP

序号	IP地址	子网掩码	端口	ARP绑定
1	192.168.23.1	255.255.255.0	Fa0/2	On

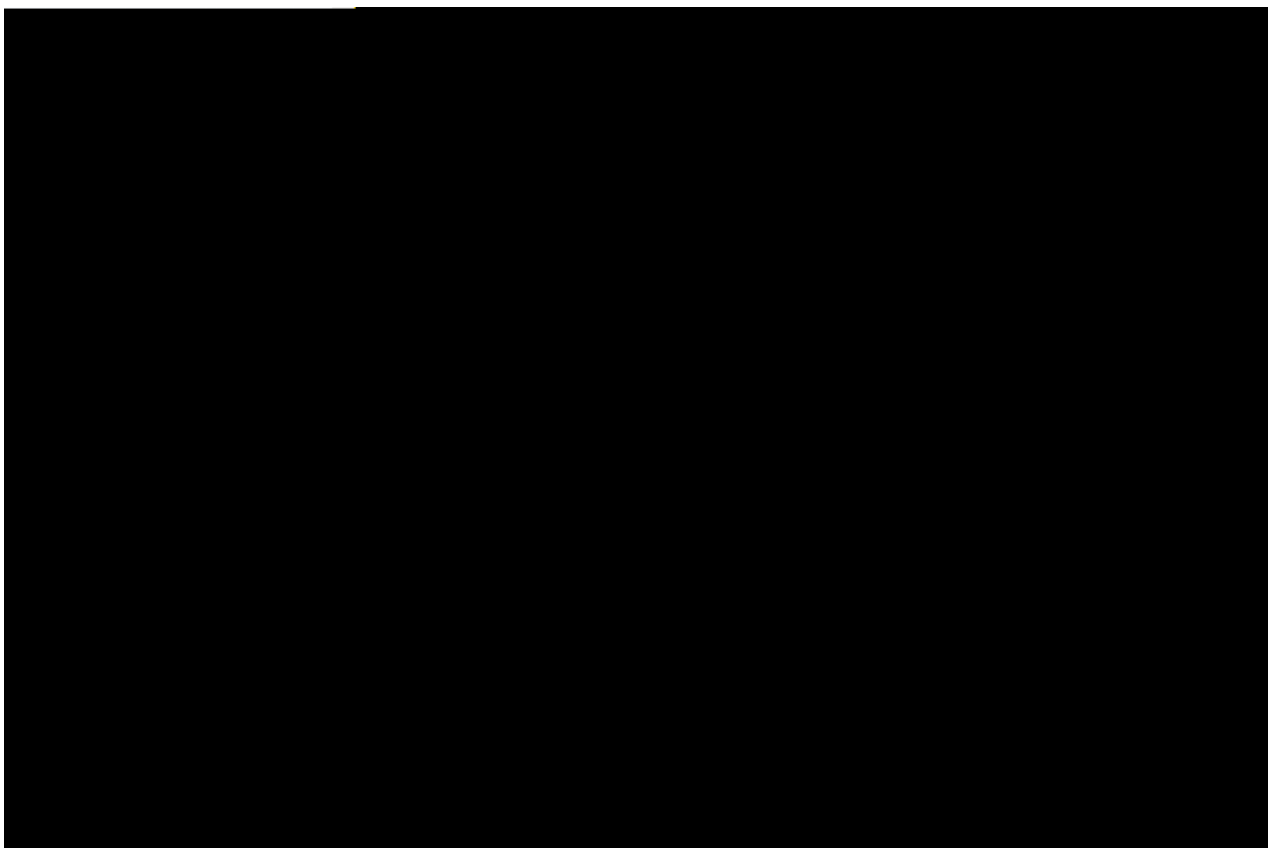
IP

1-69



" "

1-70



IP

## 1.6.14 DHCP Snooping

“ DHCP Snooping”

Snooping

1-71 DHCP Snooping

**DHCP Snooping 设置**

说明：DHCP Snooping就是DHCP窥探，通过对Client和服务器之间的DHCP交互报文进行窥探，实现对用户的监控，同时DHCP Snooping起到一个DHCP 报文过滤的功能，通过合理的配置实现对非法服务器的过滤。

保存

**DHCP Snooping 信任端口设置**

说明：由于DHCP获取IP的交互报文是使用广播的形式，因此可能存在非法服务器影响用户获取IP地址。为了防止非法服务器问题，将端口配置为两种类型，信任口和非信任口。对于DHCP客户端请求报文，仅将其转发到信任口。对于DHCP服务器响应报文，仅转发来自信任口的响应报文，而丢弃所有来自非信任口的响应报文。这样就可以实现对非法DHCP服务器的屏蔽。

端口： 保存

**DHCP Snooping配置信息**

■	端口	信任端口	限速
<div style="border: 1px solid #ccc; width: 20px; height: 20px; margin: 0 auto;"></div>			

全选
删除

DHCP Snooping

DHCP Snooping

DHCP Snooping MAC

" "

DHCP Snooping

" "

" "

## 1.7 QOS

### 1.7.1

" "

1-72



ACL

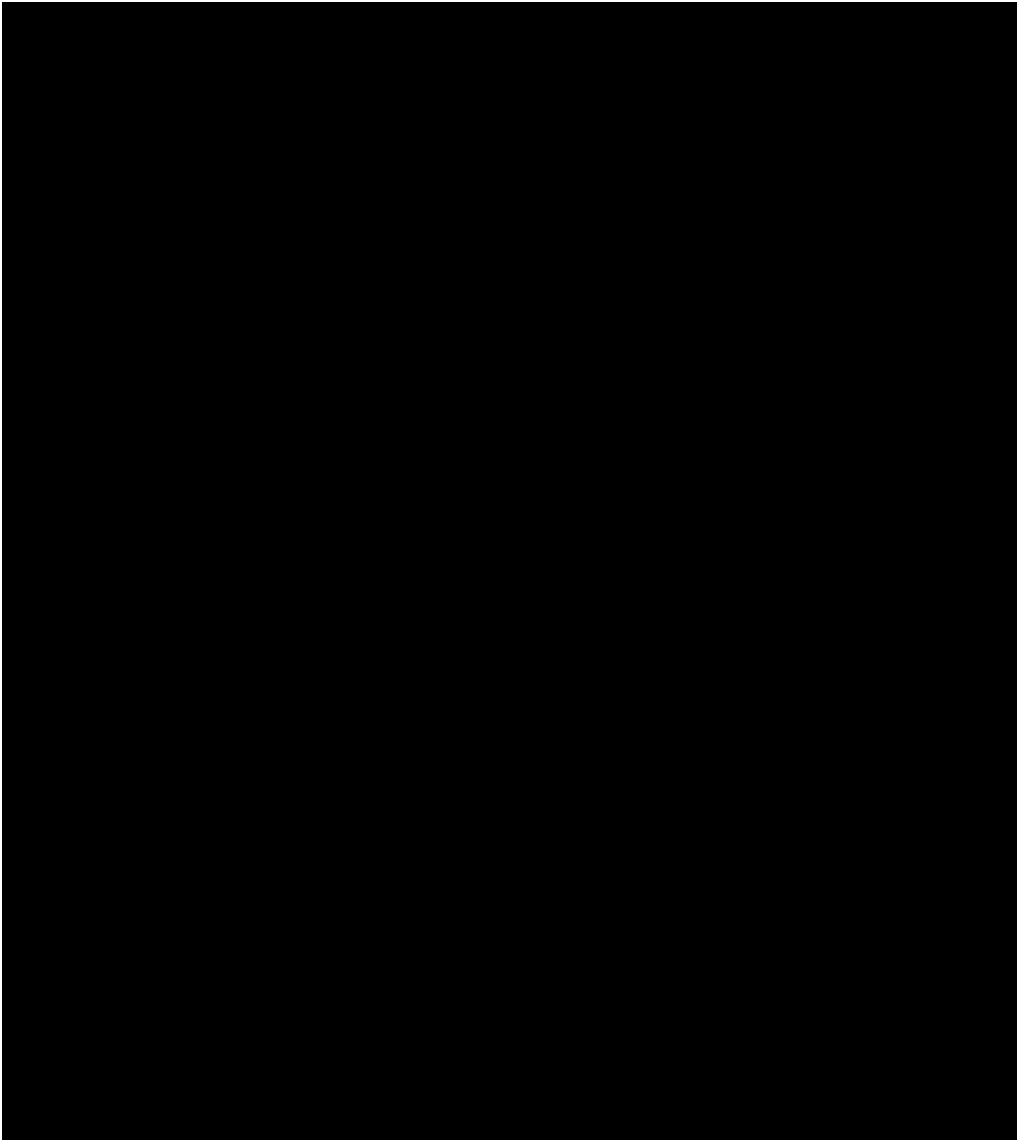
" "



### 1.7.3

" "

1-74



" "

" "

## 1.7.4

" "

1-75

将风暴控制应用于端口 (端口默认开启风暴控制)

端口:

广播

单播

(0-2147483647 可选)

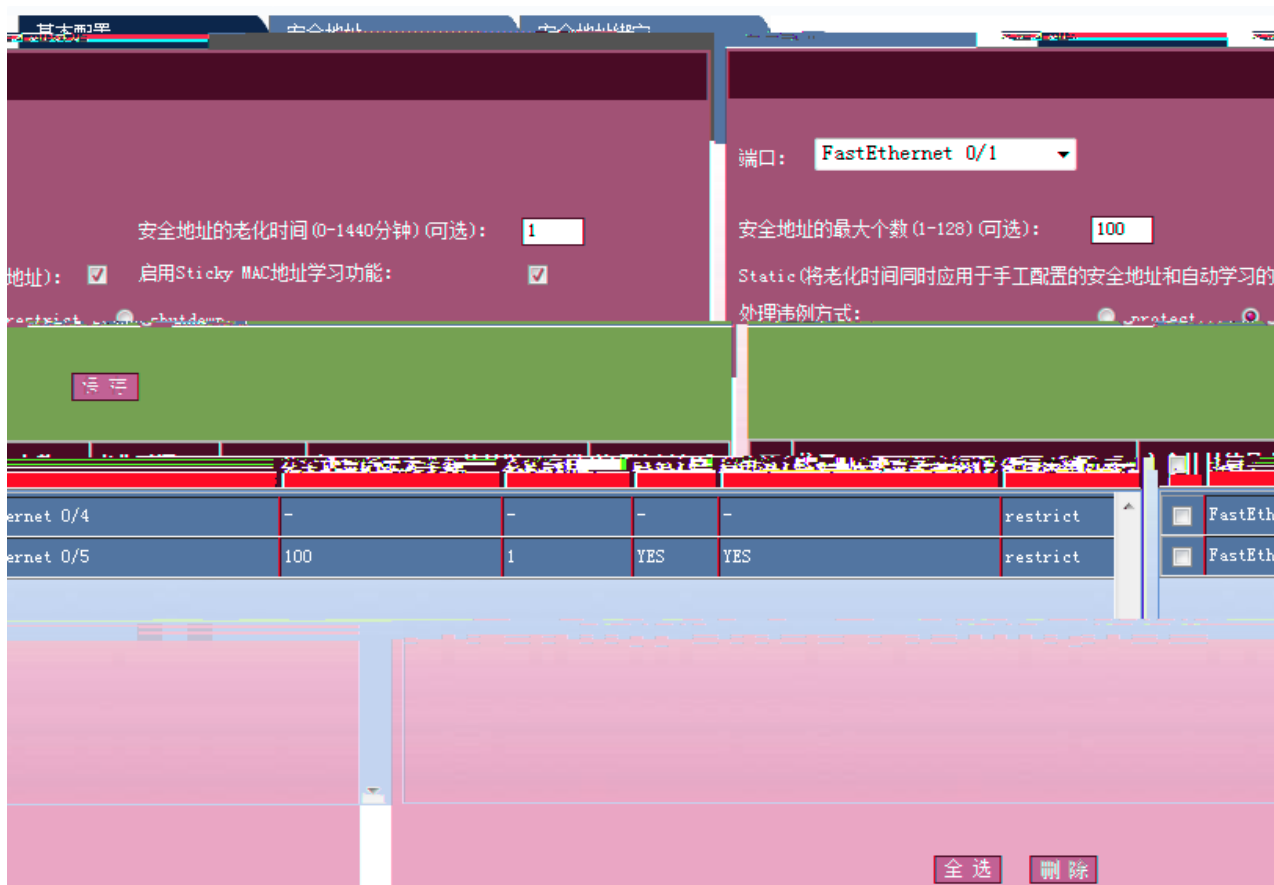
控制力度	接口	风暴类型	控制方式
-	<input type="checkbox"/> FastEthernet 0/2	broadcast	-
?	<input type="checkbox"/> FastEthernet 0/2	multicast	-
<input checked="" type="checkbox"/>	FastEthernet 0/2	unicast	level 20

" "

## 1.7.5

" "

1-76



Static      Sticky Mac



Mac VLAN ID " "

" "

基本配置    安全地址    **安全地址绑定**

端口:

IP地址 (IPv4或IPv6):

将MAC及Vlan进行绑定到安全端口:

MAC地址:       Vlan ID:

<input type="checkbox"/>	接口	MAC地址	Vlan ID	IP地址
<input checked="" type="checkbox"/>	FastEthernet 0/1	1000.0000.0000	10	1.2.3.3

Mac      VLAN ID      "      "

"      "

## 1.8

### 1.8.1

"      "

系统信息	
设备型号：	S2924G
主机名：	Ruijie
软件版本：	RGOS 10.2(4), Release(55222), Web Version:10.2.55222
硬件版本：	1.0
MAC地址：	00d0f8f80fc4

## 1.8.2

1-80

当前配置	
Building configuration...	
Current configuration : 12931 bytes	
4	2008 -
	<pre> ! version RGNOS 10.2.00(3), Release(30355) (Tue Mar 11 19:23:0 23195A44470348C) ! ! ! vlan 1  name vlan1 ! vlan 2 ! vlan 3 ! vlan 4 ! vlan 5 ! vlan 6 ! vlan 7 </pre>

## 1.8.3

1-81

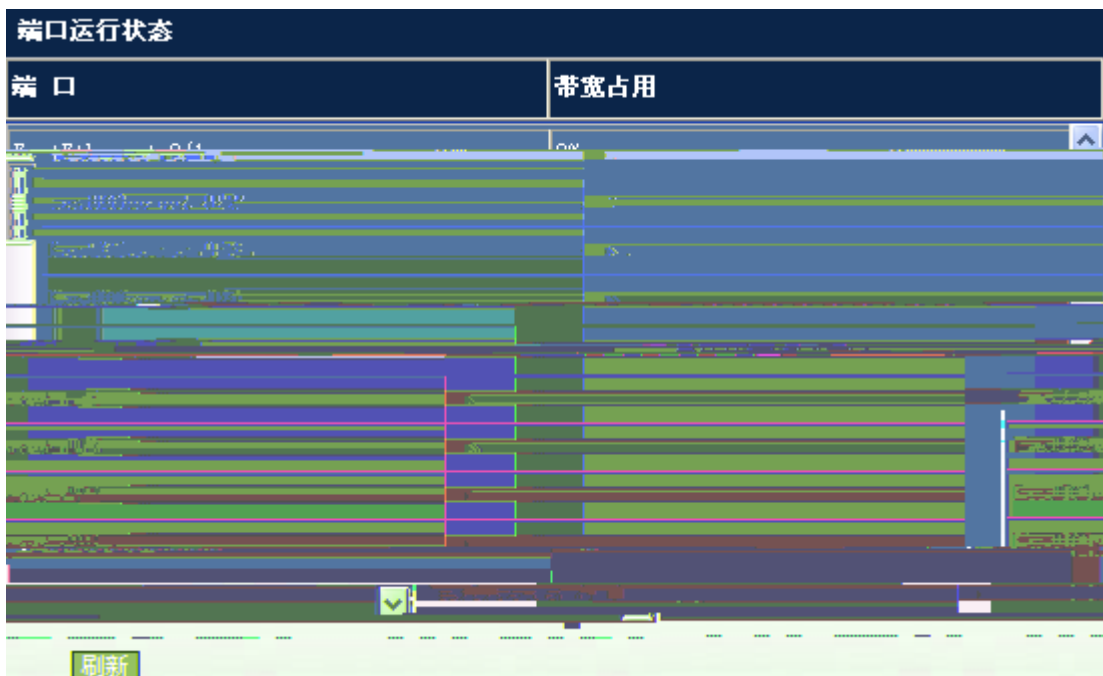
端口状态

端口	速率	类型	描述	状态	带宽
Unknown	Unknown	copper	FastEthernet 0/1	down	1
Unknown	Unknown	copper	FastEthernet 0/2	down	2
Full	100M	copper	FastEthernet 0/3	up	1
Unknown	Unknown	copper	FastEthernet 0/4	down	90
down	Unknown	copper	FastEthernet 0/5	down	1
down	Unknown	copper	FastEthernet 0/6	down	1
down	Unknown	copper	FastEthernet 0/7	down	1
down	Unknown	copper	FastEthernet 0/8	down	1
down	Unknown	copper	FastEthernet 0/9	down	1
down	Unknown	copper	FastEthernet 0/10	down	1

刷新

### 1.8.4

1-82



### 1.8.5

1-83

**端口统计信息**

注意：选择 All Ports 将统计所有接口的统计信息清零。

刷新 All Ports 清零

**输入/输出帧统计**

接收包数	发送包数	发送单播包数	发送多播包数	发送广播包数	端口	接收包数	接收单播包数	接收多播包数	接收广播包数
14043	12012	343	1688		Gi0/1	33198	8950	5508	18740
0					Gi0/2	0	0	0	0
2717					Gi0/3	2157	2146	6	5
0					Gi0/4	0	0	0	0
175					Gi0/5	34	23	11	0
0					Gi0/6	0	0	0	0
2298818					Gi0/7	882792	404167	69848	408777
0					Gi0/8	0	0	0	0
842417					Gi0/9	437082	435647	37	1398
0					Gi0/10	0	0	0	0
2367132					Gi0/11	856226	850552	149	5525
0					Gi0/12	0	0	0	0
0					Gi0/13	0	0	0	0
0					Gi0/14	0	0	0	0
8386					Gi0/15	5557815	1423231	935630	3196954
0					Gi0/16	0	0	0	0
0					Gi0/17	0	0	0	0

刷新

### 1.8.6

1-84

```

系统日志信息
Syslog logging: enabled
  Console logging: level debugging, 587 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 587 messages logged
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
Sequence-number log messages: disable
Sysname log messages: disable
Trap log messages: disable
Count log messages: disable
Trap logging: level informational, 587 messages
Log Buffer (Total: 4096 Bytes): have written 4096
ge lines logged, 0 fail
36. Overwritten 2533
*Feb 28 03:23:49: %ARP_GUARD-4-SCAN: ARP scan was detected.
*Feb 28 03:33:51: %ARP_GUARD-4-SCAN: ARP scan was detected.
*Feb 28 06:43:52: %ARP_GUARD-4-SCAN: ARP scan was detected.
*Feb 28 06:53:54: %ARP_GUARD-4-SCAN: ARP scan was detected.
*Feb 28 07:03:55: %ARP_GUARD-4-SCAN: ARP scan was detected.
*Feb 28 07:13:57: %ARP_GUARD-4-SCAN: ARP scan was detected.
*Feb 28 07:23:59: %ARP_GUARD-4-SCAN: ARP scan was detected.
*Feb 28 07:34:00: %ARP_GUARD-4-SCAN: ARP scan was detected.
*Feb 28 07:44:01: %ARP_GUARD-4-SCAN: ARP scan was detected.
*Feb 28 07:54:03: %ARP_GUARD-4-SCAN: ARP scan was detected.
*Feb 28 08:04:04: %ARP_GUARD-4-SCAN: ARP scan was detected.
*Feb 28 08:14:06: %ARP_GUARD-4-SCAN: ARP scan was detected.

```

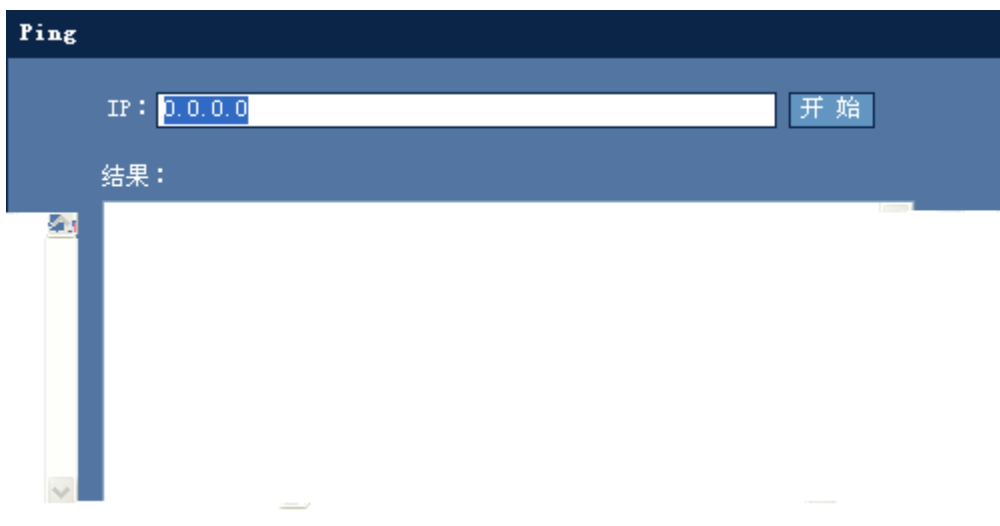
## 1.9

### 1.9.1 Ping

" Ping"

Ping

1-85 Ping



IP

" "

IP

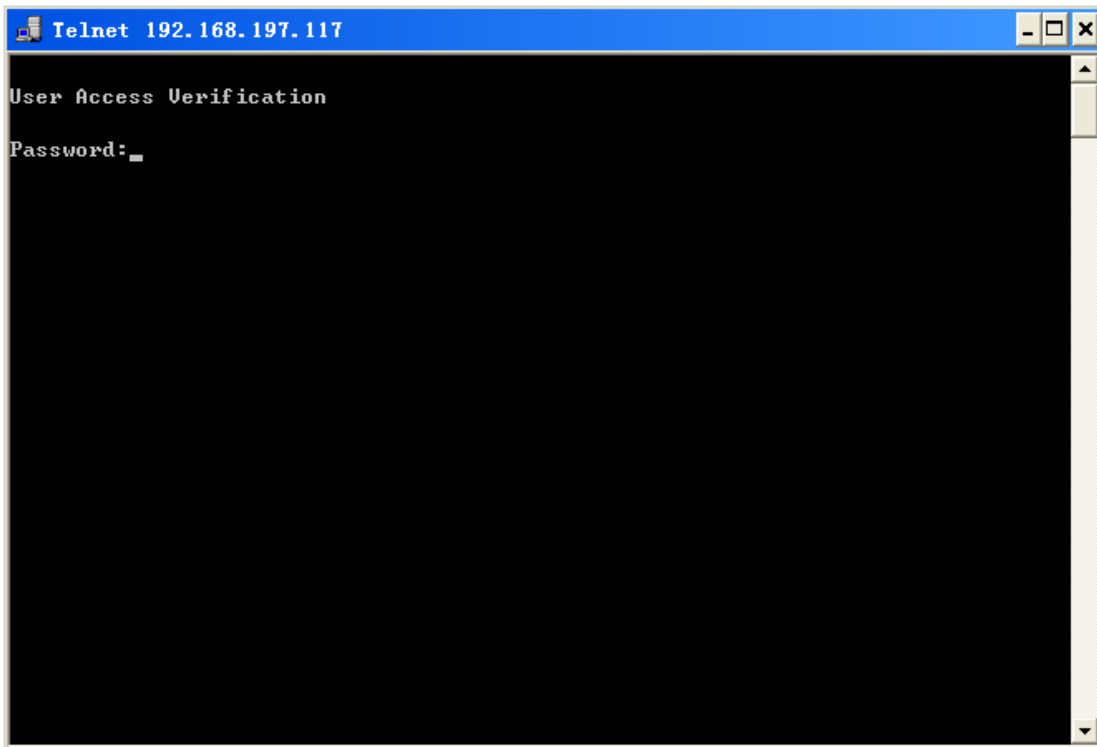
Ping

## 1.9.2 Telnet

" Telnet"

Telnet

1-86 Telnet



" Telnet"

Telnet

PC

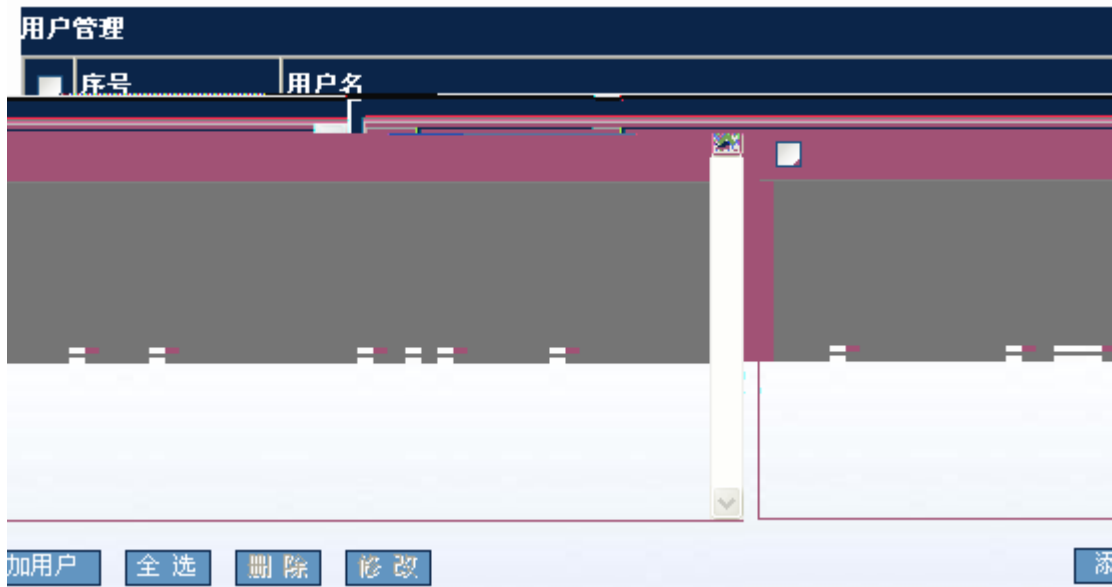
Telnet

PC Telnet

## 1.9.3

" "

1-87



1-88



1-89



Enable

Enable

1-91



Telnet

Telnet

### 1.9.5 /

" / "

/

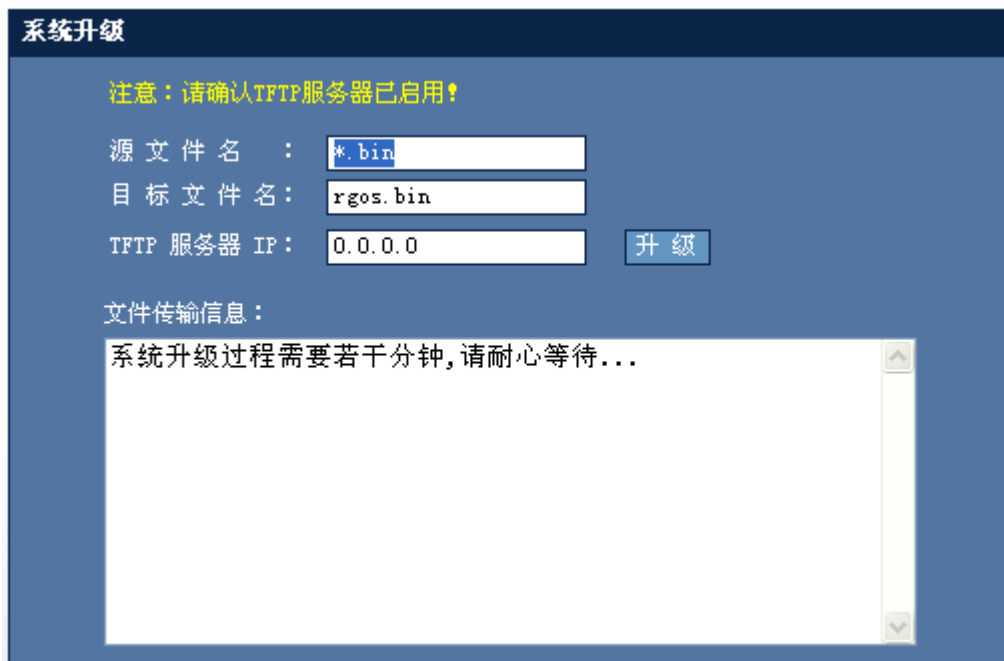
1-92 /



### 1.9.7

" "

1-94



TFTP TFTP  
TFTP IP " "

### 1.9.8

" "

" "

### 1.10 WEB

WEB WEB enable



## Local

```
Ruijie(config)#show running-config
```

```
Current configuration : 2014 bytes
```

```
!
```

```
version RGOS 10.2(4), Release(55435)(Wed May 13 11:50:07 CST 2009 -ngcf32)
```

```
vlan 1
```

```
username admin password admin //WEB
```

```
username admin privilege 15 //WEB 15
```

```
no service password-encryption
```

```
ip http authentication local //WEB local
```

```
!
```

```
enable service web-server // WEB
```

```
!
```

```
!
```

```
interface VLAN 1
```

```
no shutdown
!  
!  
line con 0  
line vty 0 4  
login  
!  
!  
end
```