



WEB

RG-S2900G-E(P)

RGOS 10.4(2b12)p6

V1.1

©2017

III

¶ ¶ ¶ ¶ ¶

¶ III



¶



¶



¶



¶



®

¶



®

¶



¶



®

¶



III

III

III

III

RGOS 10.4 (2b12)p6

-
-
-

- <http://www.ruijie.com.cn/> III
- <http://webchat.ruijie.com.cn>III
- <http://www.ruijie.com.cn/service.aspx> III
- 7 × 24 4008-111-000
- <http://support.ruijie.com.cn>
- service@ruijie.com.cn

	III á q1Vi° ·€ ëp Wñ Q¶ s < 4sAn>™ 〰

☐ ☐

III

$$\{x \mid y \mid \dots\}$$

III

 $[x | y | \dots]$

III

//

III

2)



3)

III

4

III

III

1 WEB

WEB IE
WEB WEB WEB WEB
WEB WEB IE

2 WEB

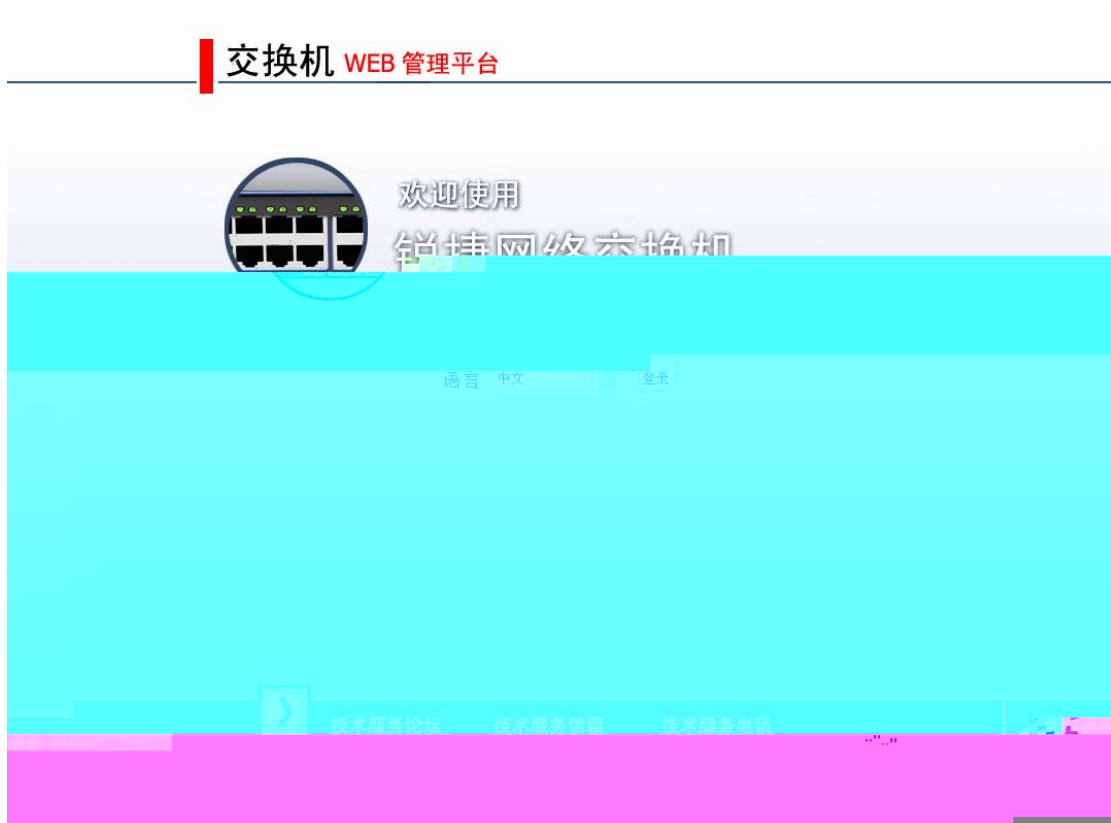
2.1

WEB

WEB	

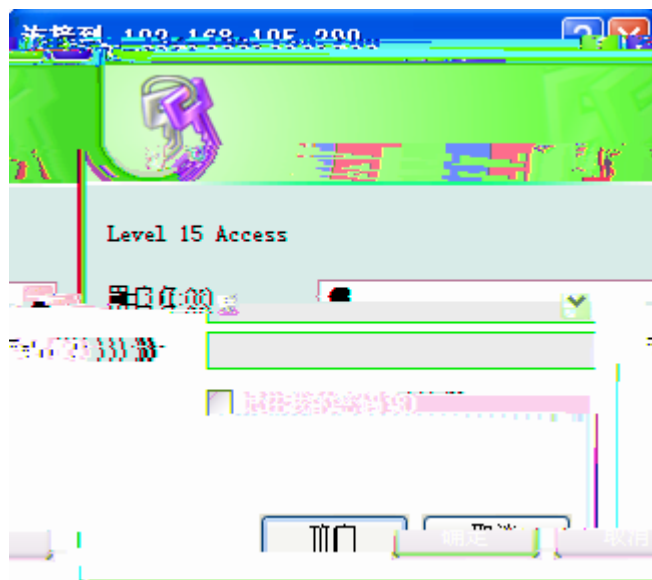
	WEB	“ WEB ”
	WEB Enable	
	Enable	

IP <http://192.168.1.200>,



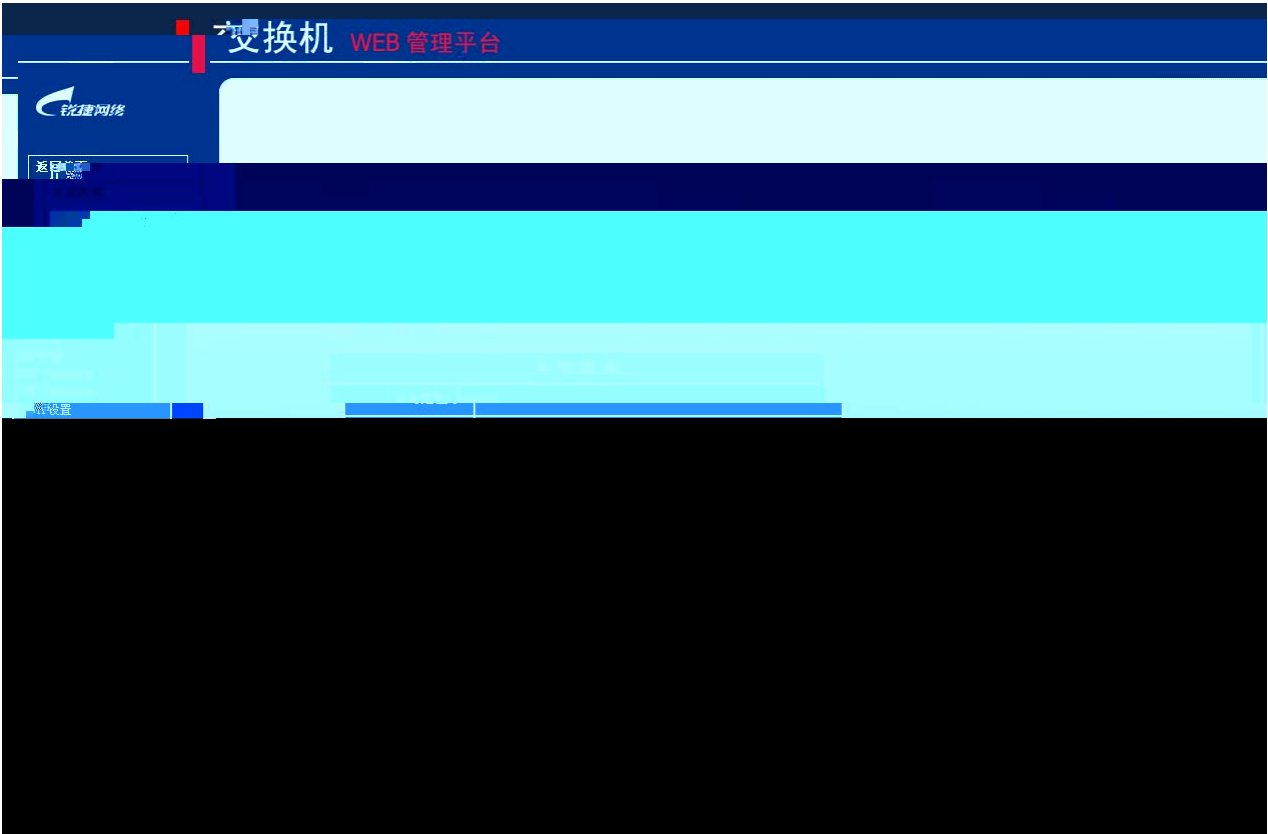
1

“ ”



2

WEB



3 WEB

	WEB	Enable
	enable	

2.2

2.2.1 IP

“ IP ”
IP

交换机IP设置

注意：如果激活交换机的IP地址，请用新的IP地址重新登录WEB。

	VLAN ID	IP地址	子网掩码	状态
☐	1	192.168.195.200	255.255.255.0	激活
☐	2	192.168.1.2	255.255.255.0	未激活

修改

4 IP

ip “ ”

交换机IP设置 -- 网页对话框

注意：如果激活修改后的VLAN，请确保激活后的VLAN的IP与网段相同。

2

192.168.1.2

255.255.255.0

☐ 激活 (UP) ☒ 未激活 (DOWN)

保存 取消

VLAN ID :

IP地址 :

子网掩码 :

激活状态 :

8.195.200/ip_mod Internet http://192.16

5 IP

IP “ ”

2.2.2 VLAN

“ VLAN ”

1 VLAN



6 VLAN

VLAN VLAN VLAN

“ ”

VLAN管理 -- 网页对话框

VLAN ID : (1-4094)

VLAN 名称 : (可选)

保存

取消

7

VLAN

VLAN ID

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

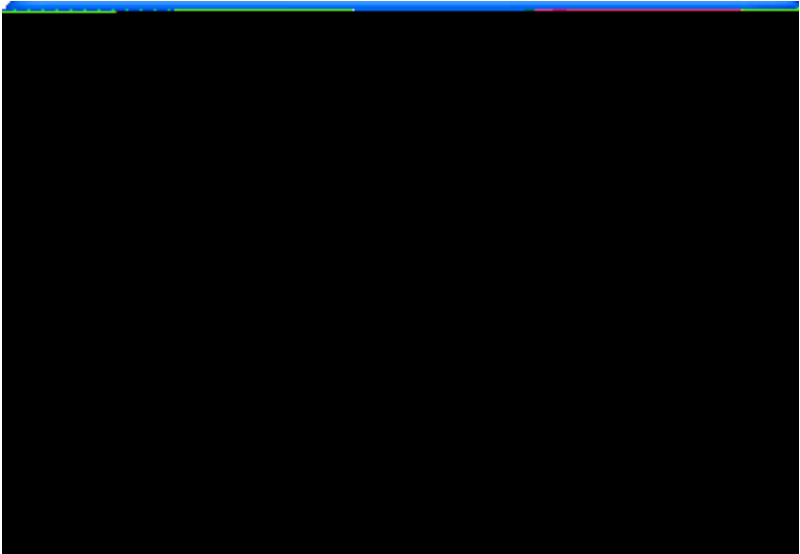
VLAN

VLAN

VLAN

VLAN

VLAN



8

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

2

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN

VLAN管理
指定VLAN

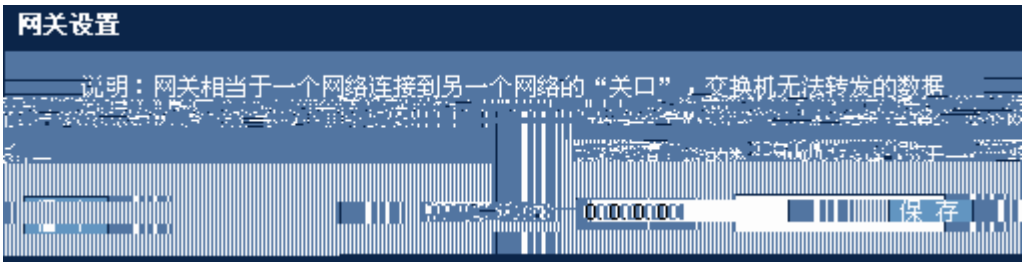
交换机端口分为两种模式：

Access模式：被模式的端口只属于一个VLAN，属于该VLAN的成员。适用于连接终端设备。

Trunk模式：被模式的端口属于多个VLAN，属于多个VLAN的成员。适用于连接交换机。

端口ID	端口名称	VLAN类型
1	GigabitEthernet 0/1	access
2	GigabitEthernet 0/1	access
3	GigabitEthernet 0/1	access
4	GigabitEthernet 0/1	access
5	GigabitEthernet 0/1	access
6	GigabitEthernet 0/1	access
7	GigabitEthernet 0/1	access
8	GigabitEthernet 0/1	access
9	GigabitEthernet 0/1	access
10	GigabitEthernet 0/1	access
11	GigabitEthernet 0/1	access
12	GigabitEthernet 0/1	access
13	GigabitEthernet 0/1	access
14	GigabitEthernet 0/1	access
15	GigabitEthernet 0/1	access

保存

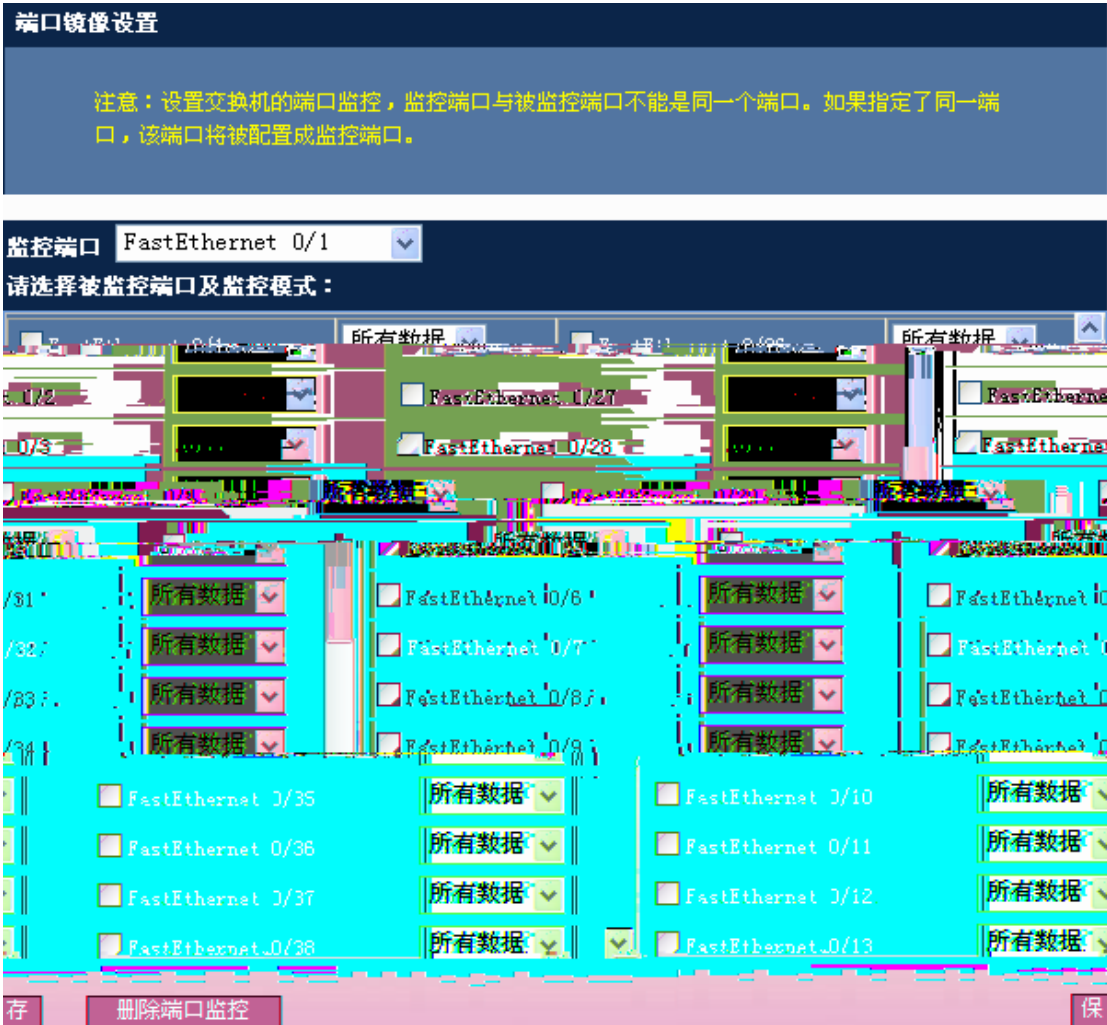


10

IP IP “ ”

2.2.4

“ ”



11

“ ”

“ ”

2.2.5

“ ”

端口限速设置

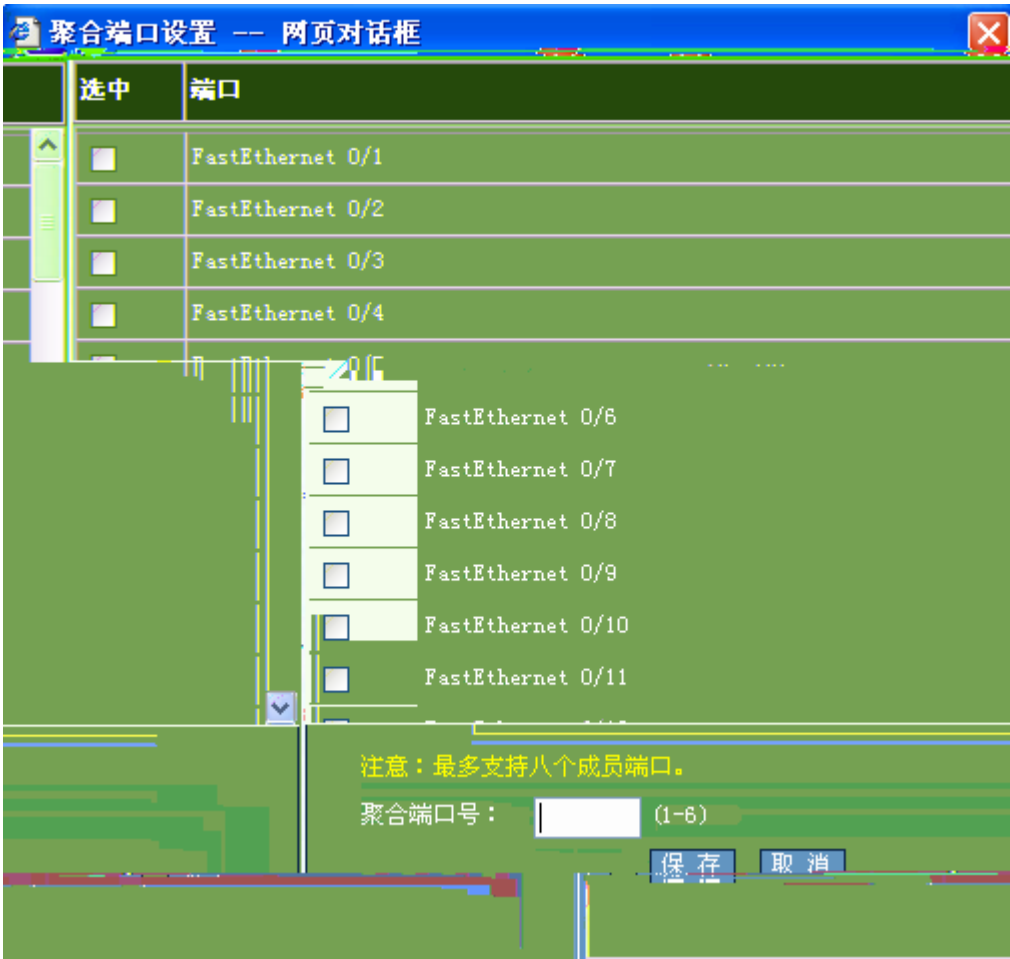
注意：不限速的端口，保持对应文本框为空（1byte=8bit）。S2900系列设备不支持对端口输入速率限制的设置。

端口	输出速率限制 (312-1000000 KBit/s)	输入速率限制 (312-1000000 KBit/s)
GigabitEthernet 0/1		
GigabitEthernet 0/2		
GigabitEthernet 0/3		
GigabitEthernet 0/4		
GigabitEthernet 0/5		
GigabitEthernet 0/6		
GigabitEthernet 0/7		
GigabitEthernet 0/8		
GigabitEthernet 0/9		
GigabitEthernet 0/10		
GigabitEthernet 0/11		
GigabitEthernet 0/12		
GigabitEthernet 0/13		
GigabitEthernet 0/14		
GigabitEthernet 0/15		

12

“ ”
“ ”

2.2.6 101Dc 9230.04 62E09DC6309B7004192354202TE494D3660739D662AF31B1C00



14

“ ”

3

“ ”

2.2.7

“ ”



15

“ ”

2.2.8 DHCP

“ DHCP ”

DHCP

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

保存

DHCP服务器设置

DHCP服务器：

0.0.0.0

保存

DHCP服务器

16 DHCP

1) / DHCP

/ DHCP

“ ”

2)DHCP

DHCP

“ ”

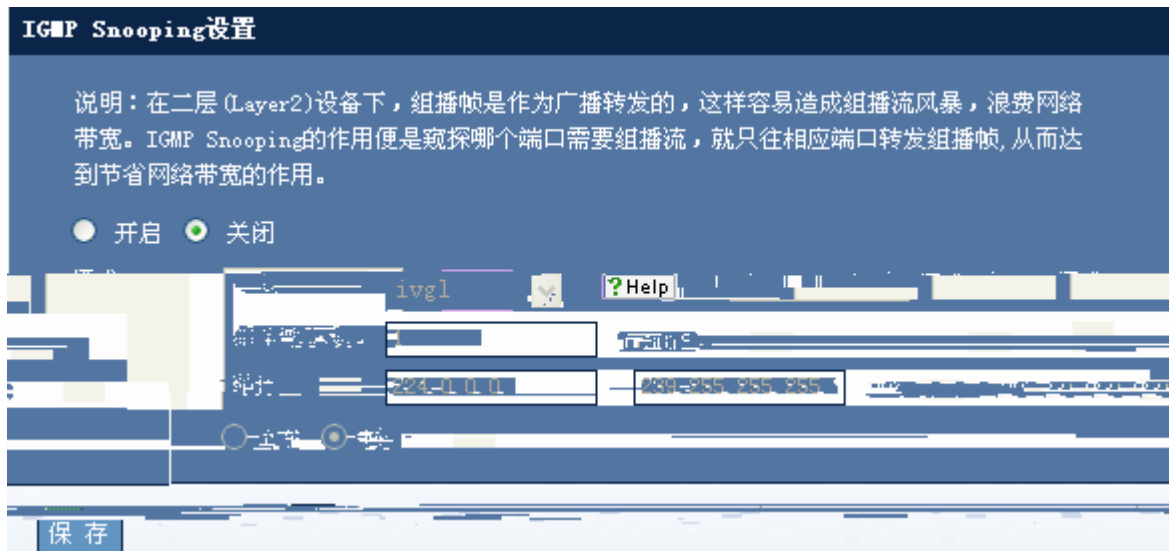
DHCP

“ ”

2.2.9 IGMP Snooping

“ IGMP Snooping ”

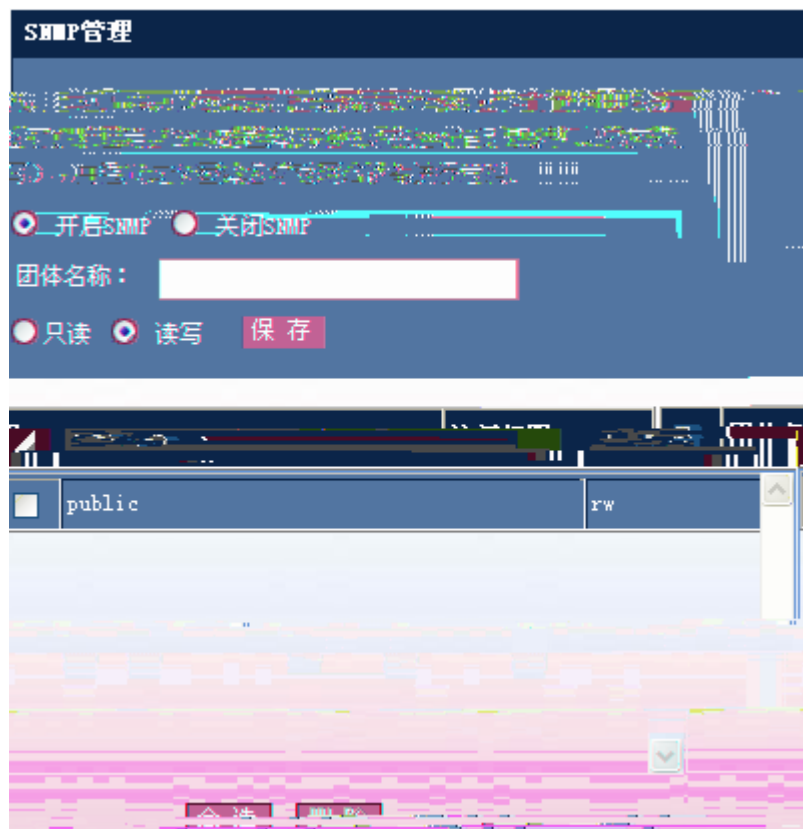
IGMP Snooping



17 IGMP Snooping

I e ^ i “ ”

SNMP



19 SNMP

SNMP

“

SNMP”

“

”

SNMP

“

SNMP”

“

”

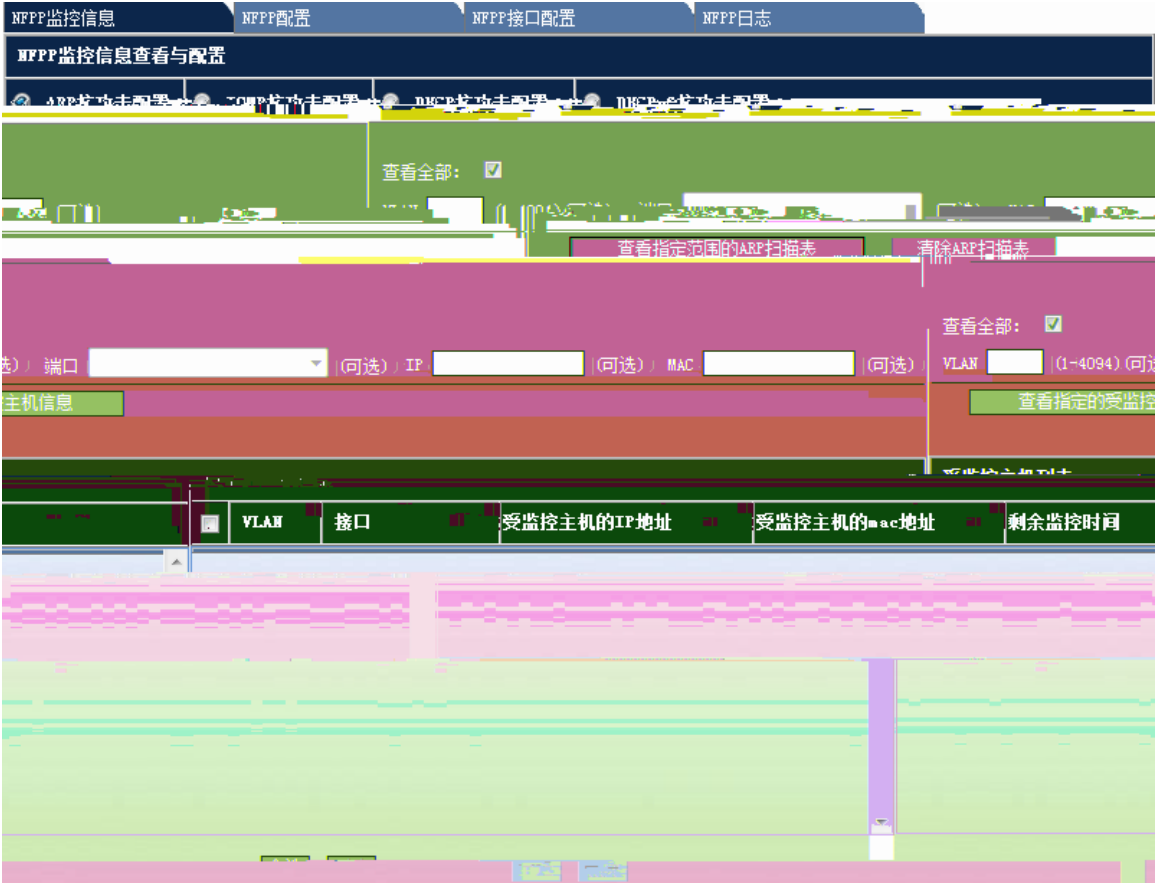
“

”

2.2.12 NFPP

“NFPP”

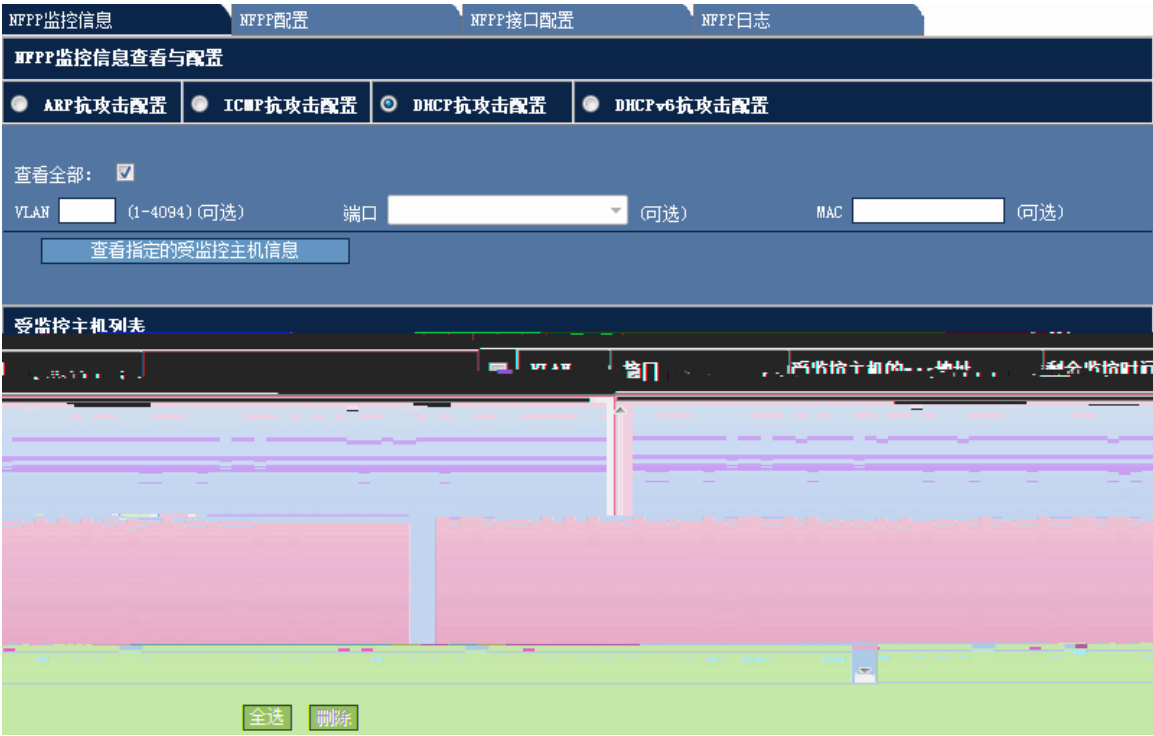
1 NFPP



20 NFPP

- ARP

WEB



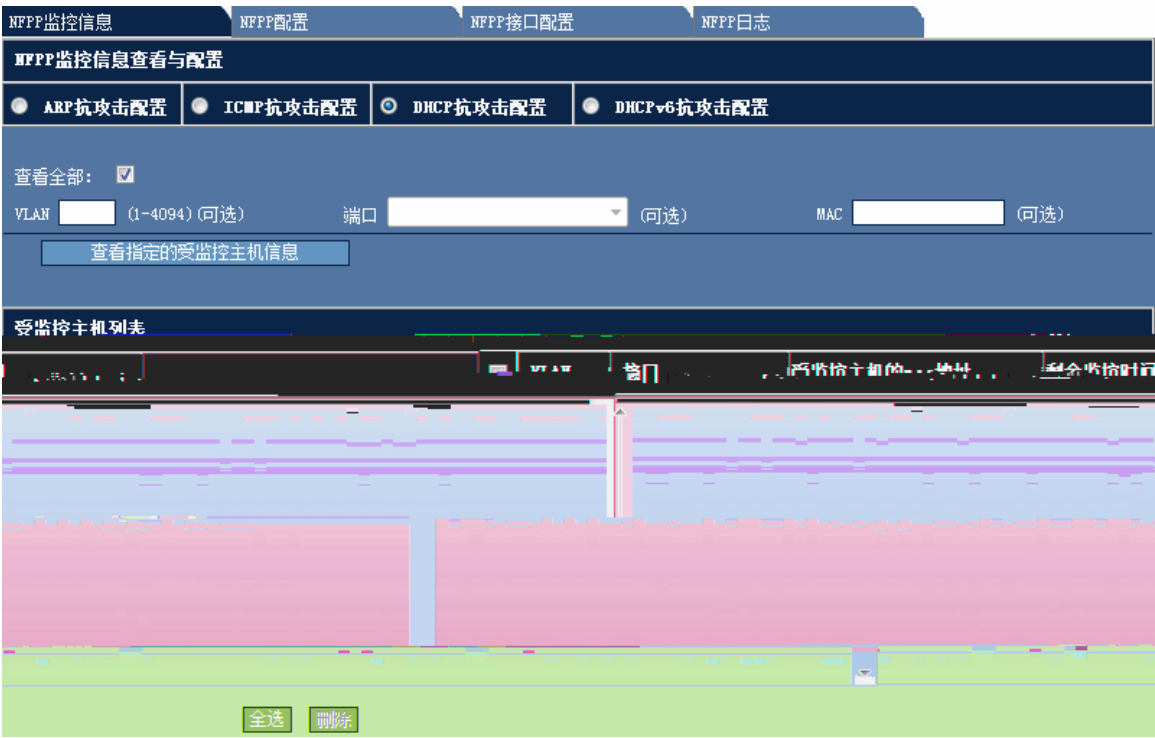
23 NFPP —DHCP

DHCP

“ ”

“ ”

- DHCPv6



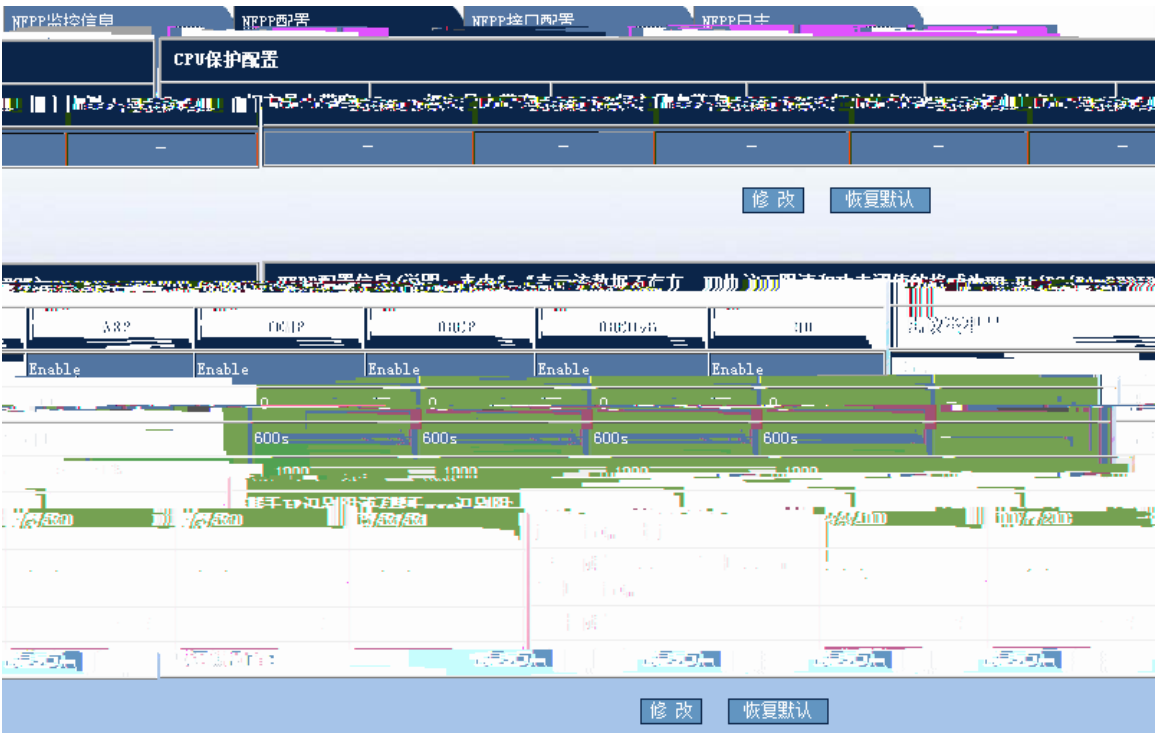
24 NFPP —DHCP

DHCPv6

“ ”

“ ”

2 NFPP

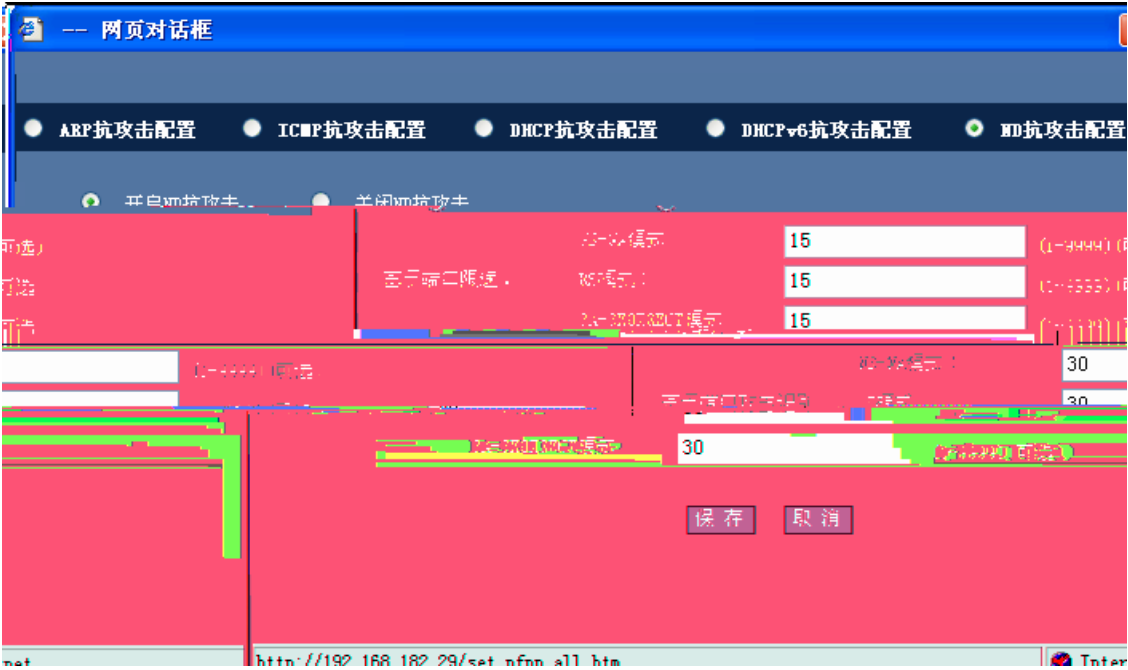


25 NFPP —DHCPv6
CPU



26 CPU

- CPU “ ”
- NFPP “ ”



27 NFPP



3 NFPP

- ARP

NFPP监控信息NFPP配置NFPP接口配置NFPP日志

NFPP接口信息配置

ICMP抗攻击配置

DHCP抗攻击配置

DHCPv6抗攻击配置

ND抗攻击配置

ARP抗攻击配置

0/1

开启ARP抗攻击

关闭ARP抗攻击

默认

接口: FastEthernet

基于ip/vid/端口识别主机

基于mac/vid/端口识别主机

基于port端口识别主机(可

隔离时间: 123

(可选): 限速值: 123 (1-9999) 攻击阈值: 123 (1-9999)

限速值: 789 (1-9999) 攻击阈值: 789 (1-9999)

限速值: 123 (1-9999) 攻击阈值: 456 (1-9999)

(0/30-86400) (可选) 永久隔离 扫描阈值: 123 (1-9999) (可选)

保存

攻击状态	隔离时间	限速值 (基于IP/MAC/PORT)	攻击阈值 (基于IP/MAC/PORT)	扫描阈值	接口	ARP抗攻击
	123	123/789/123	123/789/456	123	Fa0/1	Enable

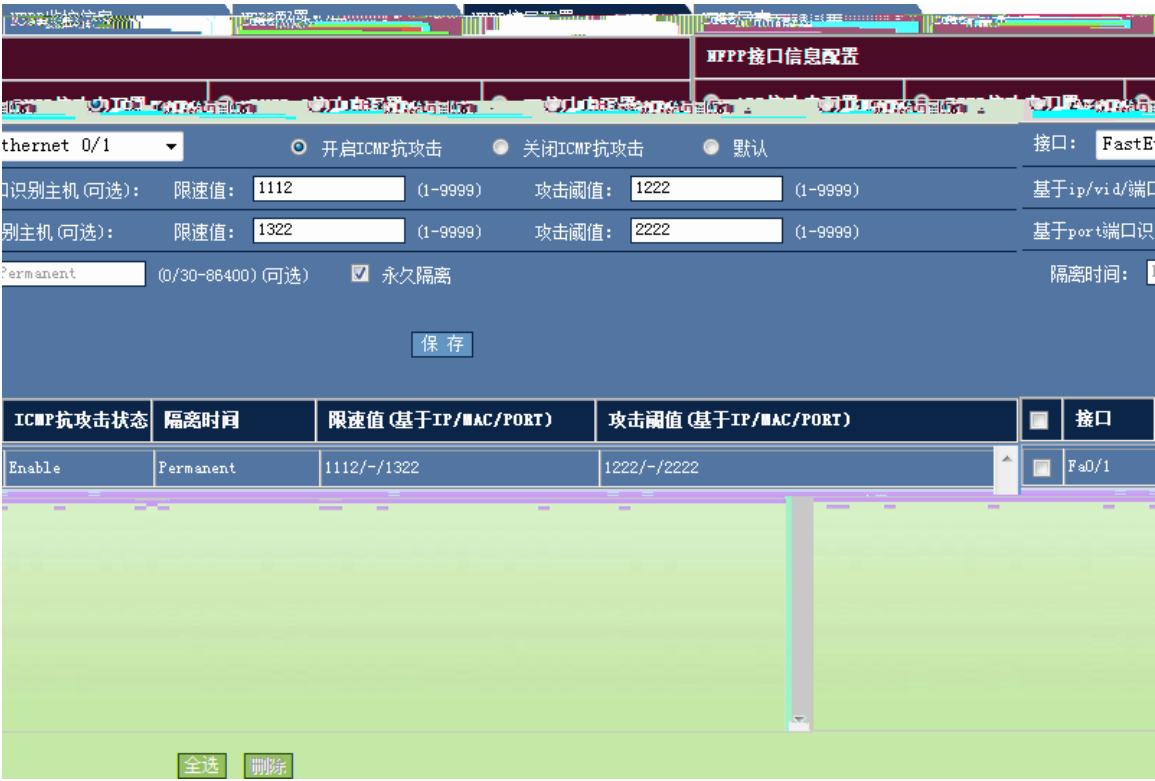
全选

删除

28 NFPP —NFPP ARP

ARP “ ”

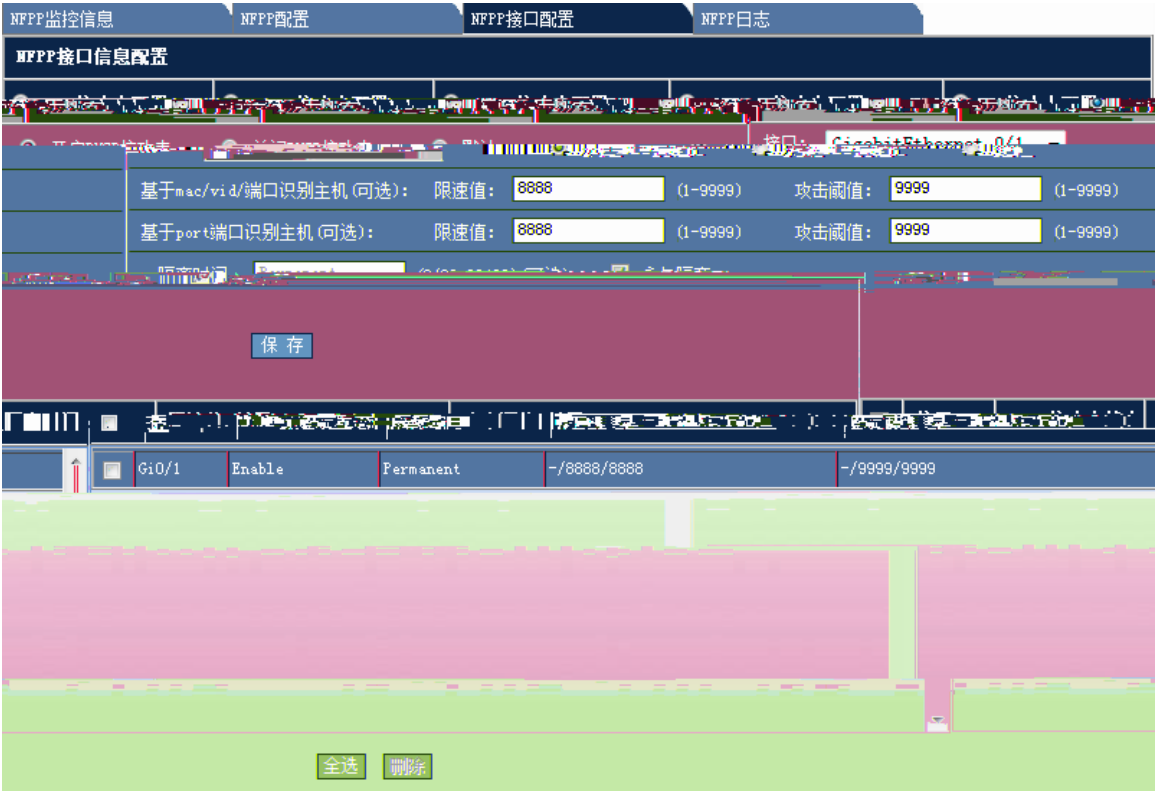
- ICMP



29 NFPP —NFPP ICMP

ICMP “ ” NFPP

- DHCP



30 NFPP —NFPP DHCP

DHCP “ ” NFPP

- DHCPv6

NFPP监控信息

NFPP配置

NFPP接口配置

NFPP日志

抗攻击配置

ND抗攻击配置

攻击

默认

9999

(1-9999)

9999

(1-9999)

NFPP接口信息配置

ARP抗攻击配置

ICMP抗攻击配置

DHCP抗攻击配置

DHCPv6抗攻击配置

接口: GigabitEthernet 0/1

开启DHCPv6抗攻击

关闭DHCPv6抗攻击

基于mac/vid/端口识别主机(可选): 限速值: 8888 (1-9999) 攻击阈值:

基于port端口识别主机(可选): 限速值: 8888 (1-9999) 攻击阈值:

隔离时间: Permanent (0/30-86400)(可选) ☒ 永久隔离

保存

MAC(PORT)	接口	DHCPv6抗攻击状态	隔离时间	限速值(基于IP/MAC/PORT)	攻击阈值(基于IP/MAC/PORT)
	☒ Gi0/1	Enable	Permanent	-/8888/8888	-/9999/9999

全选

删除

31 NFPP —NFPP DHCPv6

DHCPv6 “ ”

- ND

NFPP监控信息

NFPP配置

NFPP接口配置

NFPP日志

NFPP接口信息配置

☒ ARP攻击配置

☐ ICMP攻击配置

☐ DHCP攻击配置

☐ DHCPv6攻击配置

☒ DD攻击配置

Cisco-Ethernet_0/1

限速度：8888(1-9999)

攻击阈值：9999(1-9999)

NS-NA模式：

限速值：1111(1-9999)

攻击阈值：2222(1-9999)

基于源IP地址识别主机(勾选)：

限速值：3333

攻击阈值：5555

保存

接口名称

接口描述

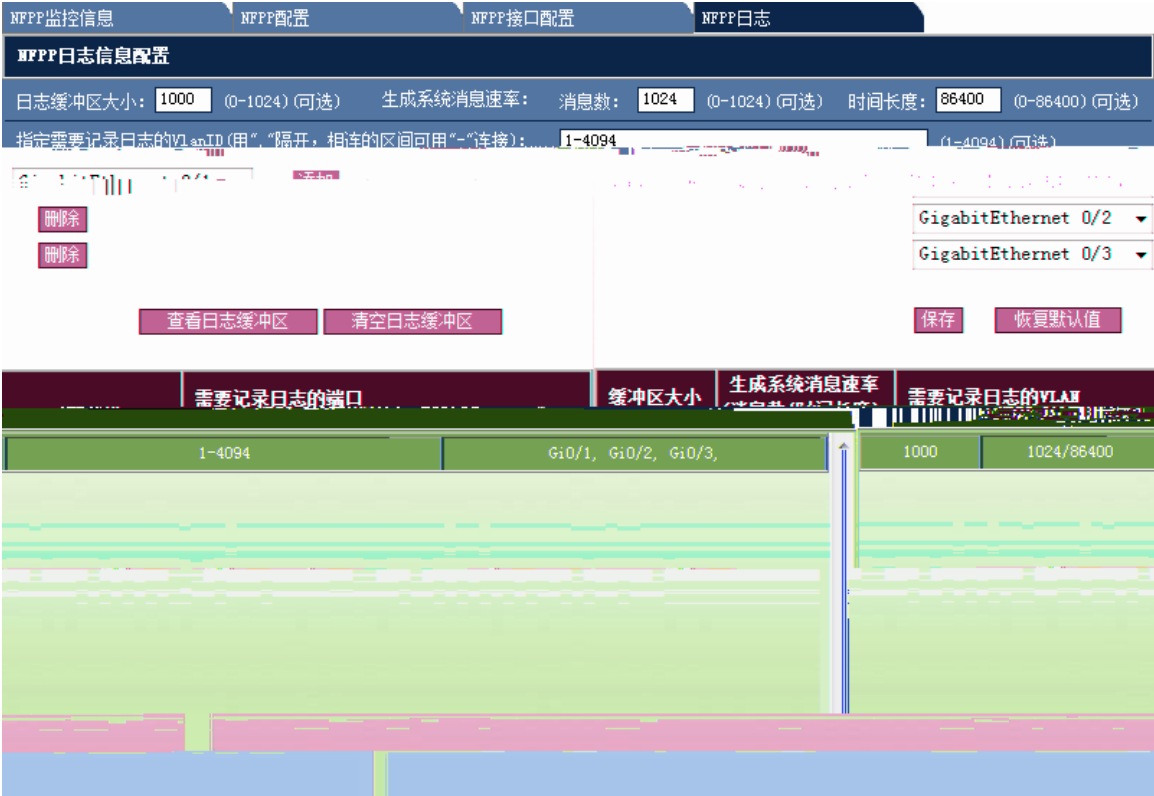
接口类型

接口状态

GigabitEthernet0/1	Enable	8888/1111/3333	9999/2222/5555
--------------------	--------	----------------	----------------

全选

删除



33 NFPP

NFPP

“ ”

“ ”

“ ”

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)

指定需要记录日志的VLAN (用“|”隔开，指定的区间可用“-”连接)： (0-4094) (可选) =

Configuration Process

Configuration Process

保存

恢复默认值

查看日志缓冲区

清空日志缓冲区

日志缓冲区：

Protocol	VLAN	Interface	IP address	MAC address	Reason	Timestamp
----------	------	-----------	------------	-------------	--------	-----------

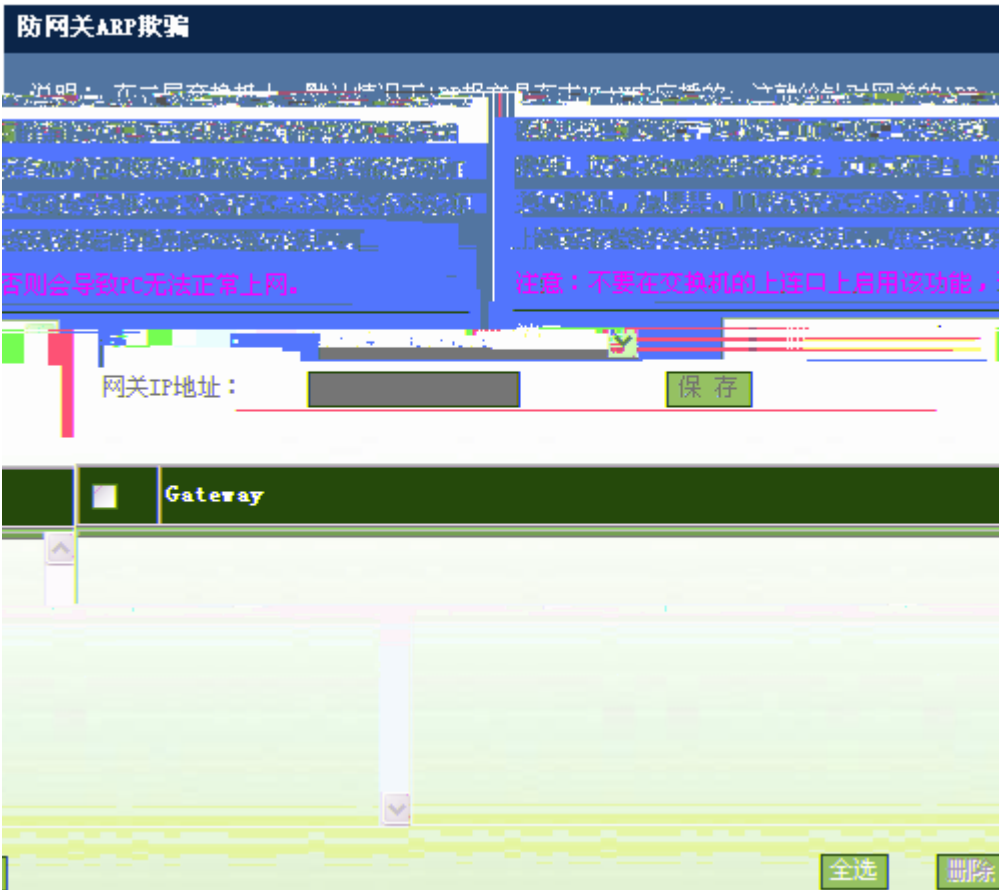
34

2.3

2.3.1 ARP

“ ARP ”

ARP



35 ARP

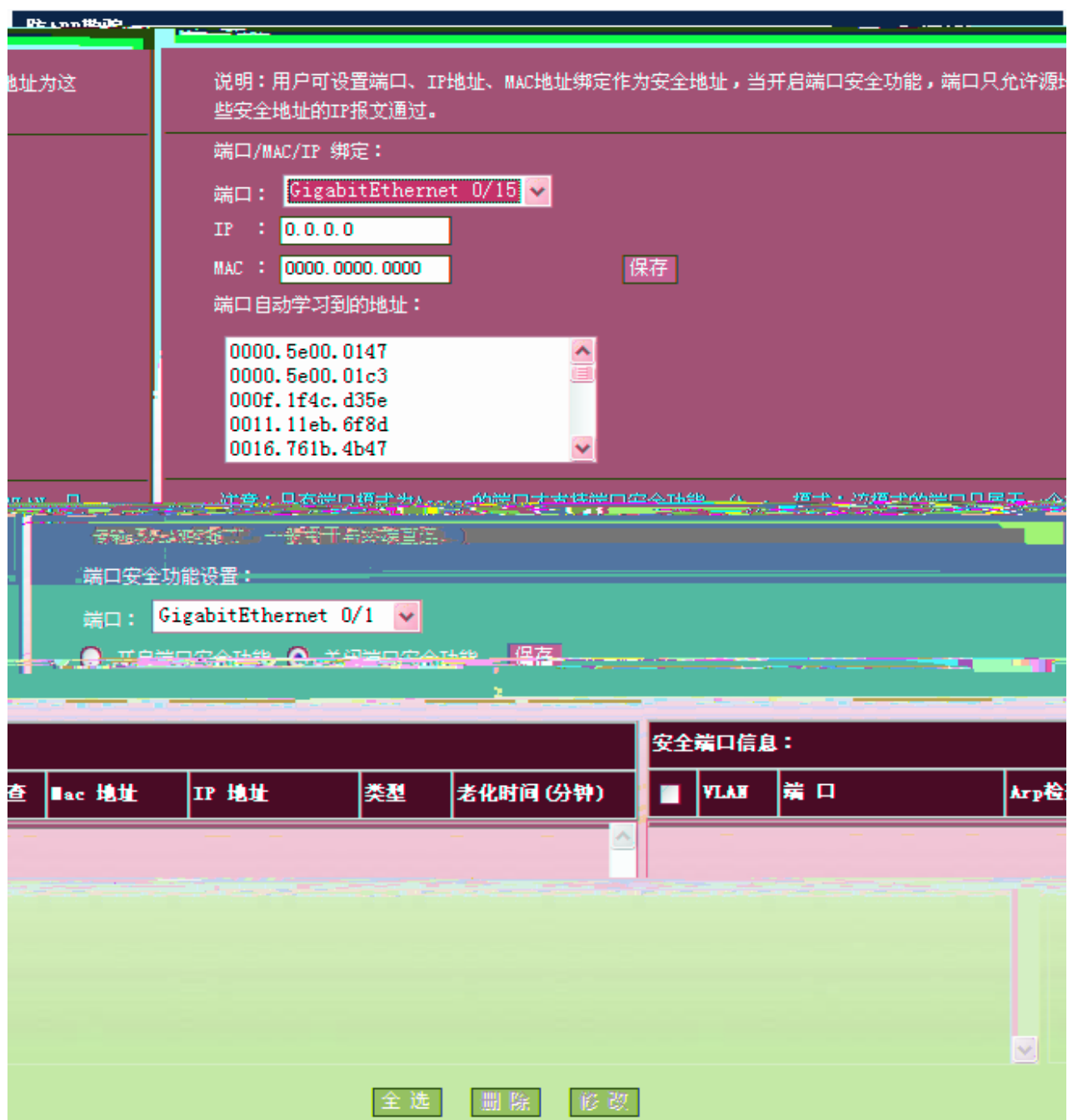
“ ”

“ ”

2.3.2 ARP

“ ARP ”

ARP



36 ARP

1) /MAC/IP

“ /MAC/IP ”

MAC

GigabitEthernet 0/15

MAC

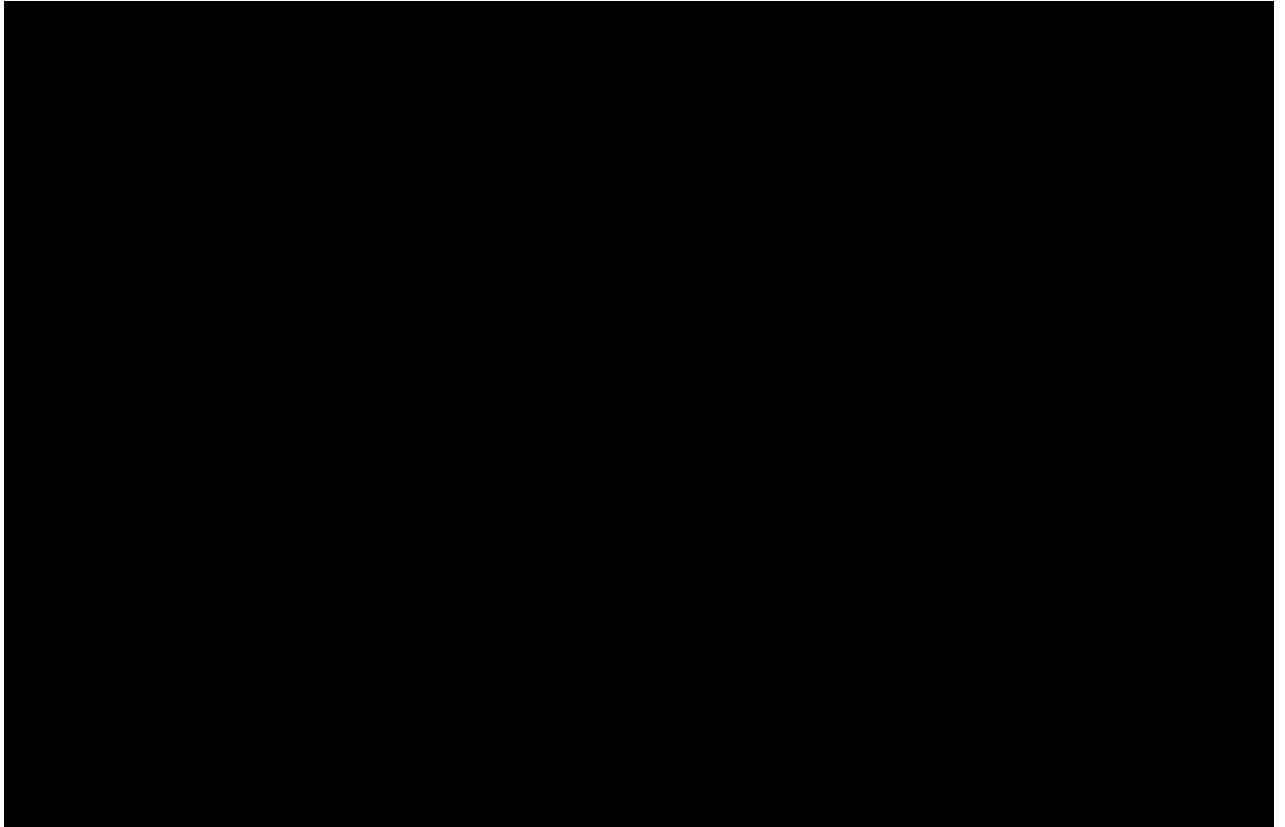
2

3)

2.3.4 ACL

“ ACL ”

ACL



39 ACL

1 ACL

ACL

ACL

“

”

ACE

“

”

2 ACL

IP

“

IP

”

IP

ACL

ACE

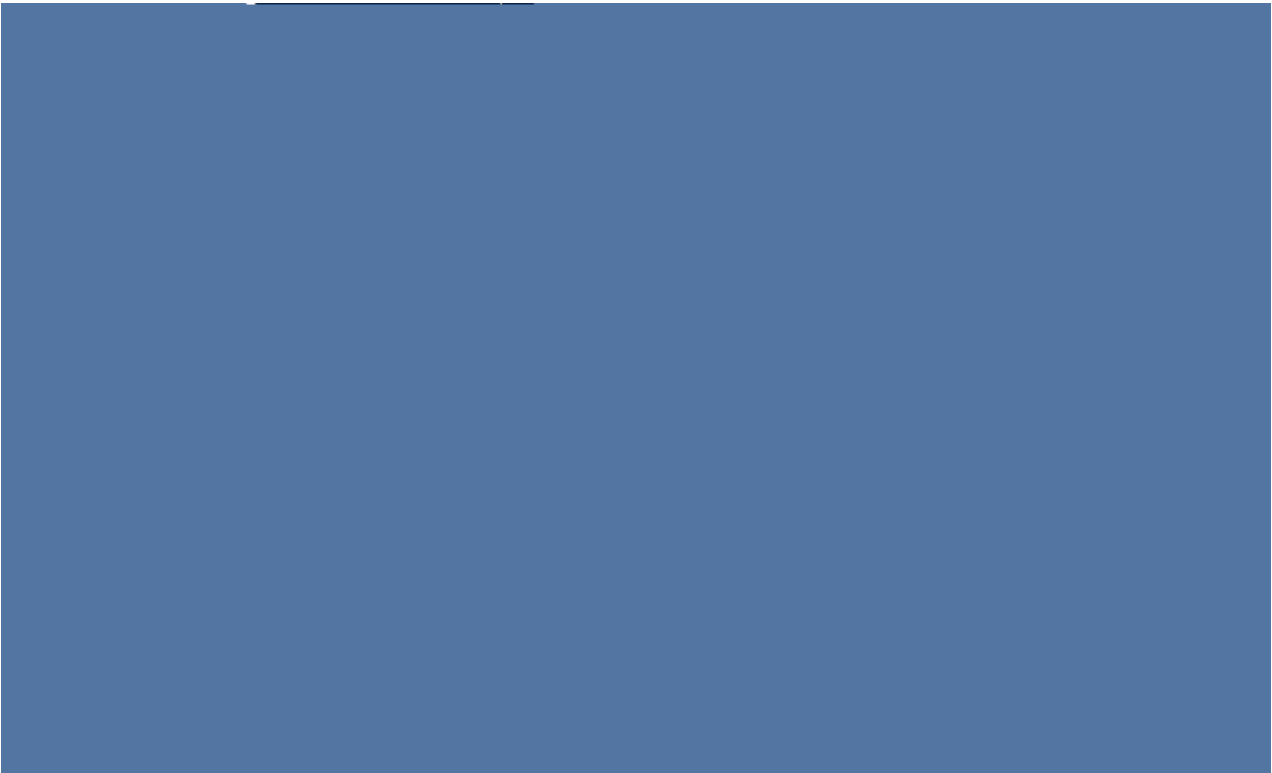
ACL

ACE

ACL

“

”



40 IP

“ ” “ ”

ID

IP

IP

,

IP

“

”

IP

“

IP

”

IP

The screenshot displays the ACL configuration page. At the top, there are tabs for '显示ACL信息' (Show ACL Information), 'ACL配置' (ACL Configuration), and '将ACL应用于端口' (Apply ACL to Port). The 'ACL配置' tab is active. Below the tabs, there is a configuration table with the following columns: 规则名 (Rule Name), 动作 (Action), 协议 (Protocol), 源IP地址 (Source IP Address), and 目的IP地址 (Destination IP Address). The first rule is named '禁止' (Prohibit) and has the action '禁止' (Prohibit). The protocol is set to 'TCP'. The source IP address is '0.0.0.0' and the destination IP address is '0.0.0.0'. At the bottom right, there is a '保存' (Save) button.

41 IP

“ ” “ ”

ID

TCP UDP IP ICMP

IP

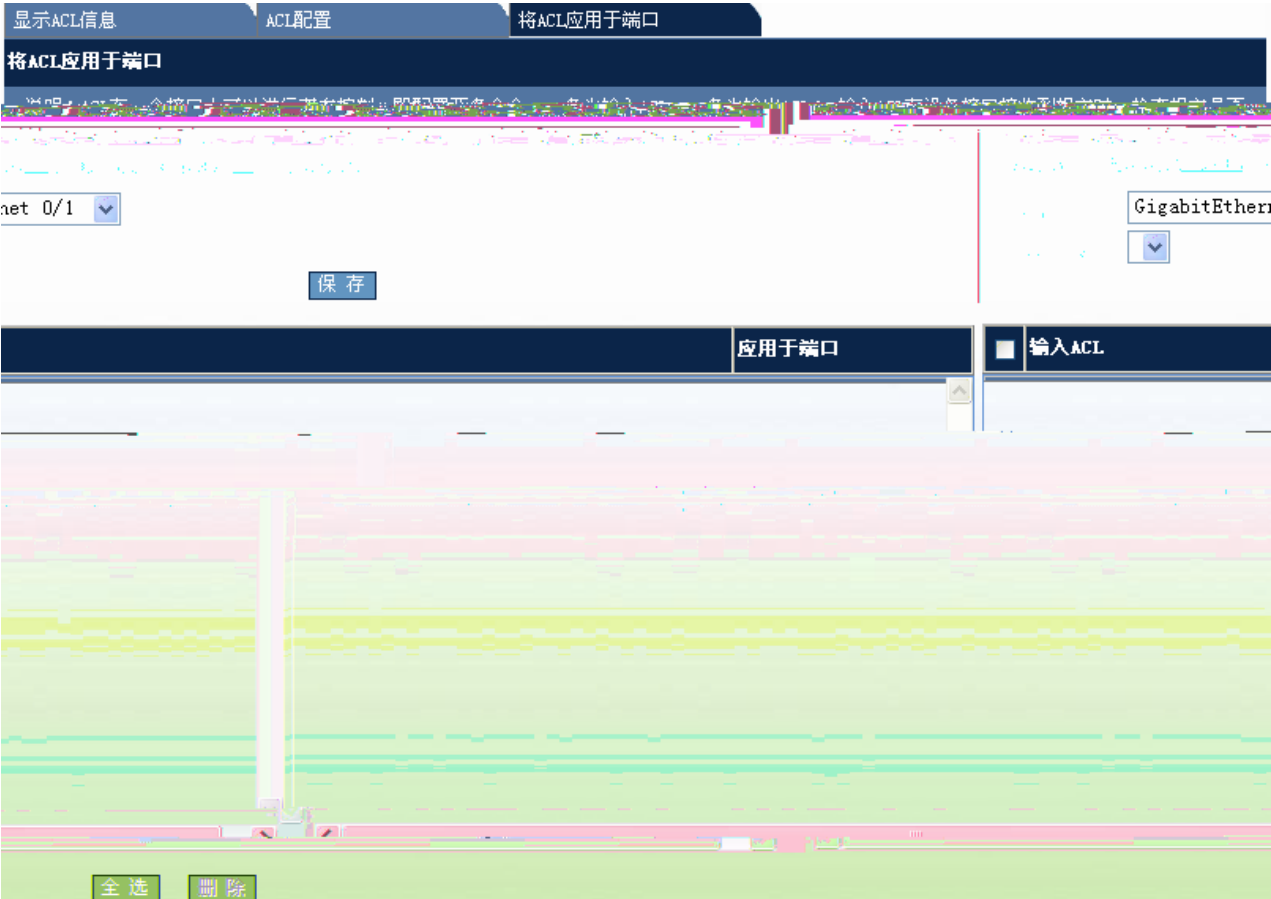
IP

IP

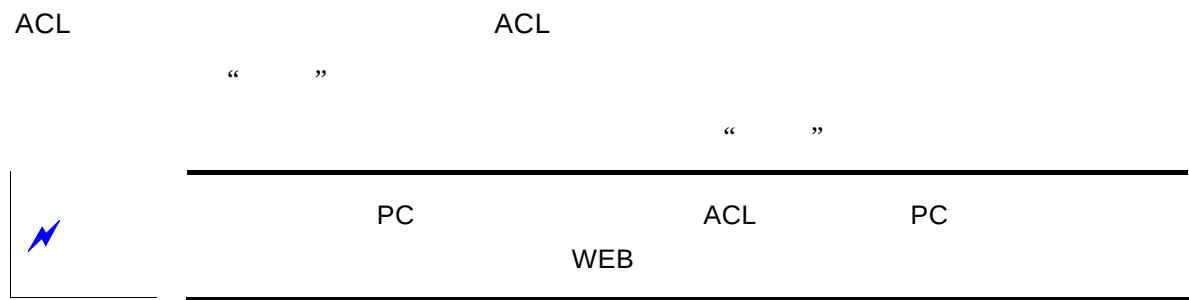
IP

IP

IP



42 ACL



2.3.5 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



43 IP Source Guard

1

IP Source Guard

IP+MAC “ IP+MAC ()”

2

IP

MAC

MAC

VLAN

VLAN ID

IP

IP

接口配置

用户绑定

配置静态的IP源地址绑定用户

MAC地址:

VLAN:

(1-4094)

IP地址:

选择接口:

保存

MAC地址	IP地址	租期	类型	VLAN	接口

删除

全选

44

2.3.6 DAI

DAI

Dynamic ARP Inspection

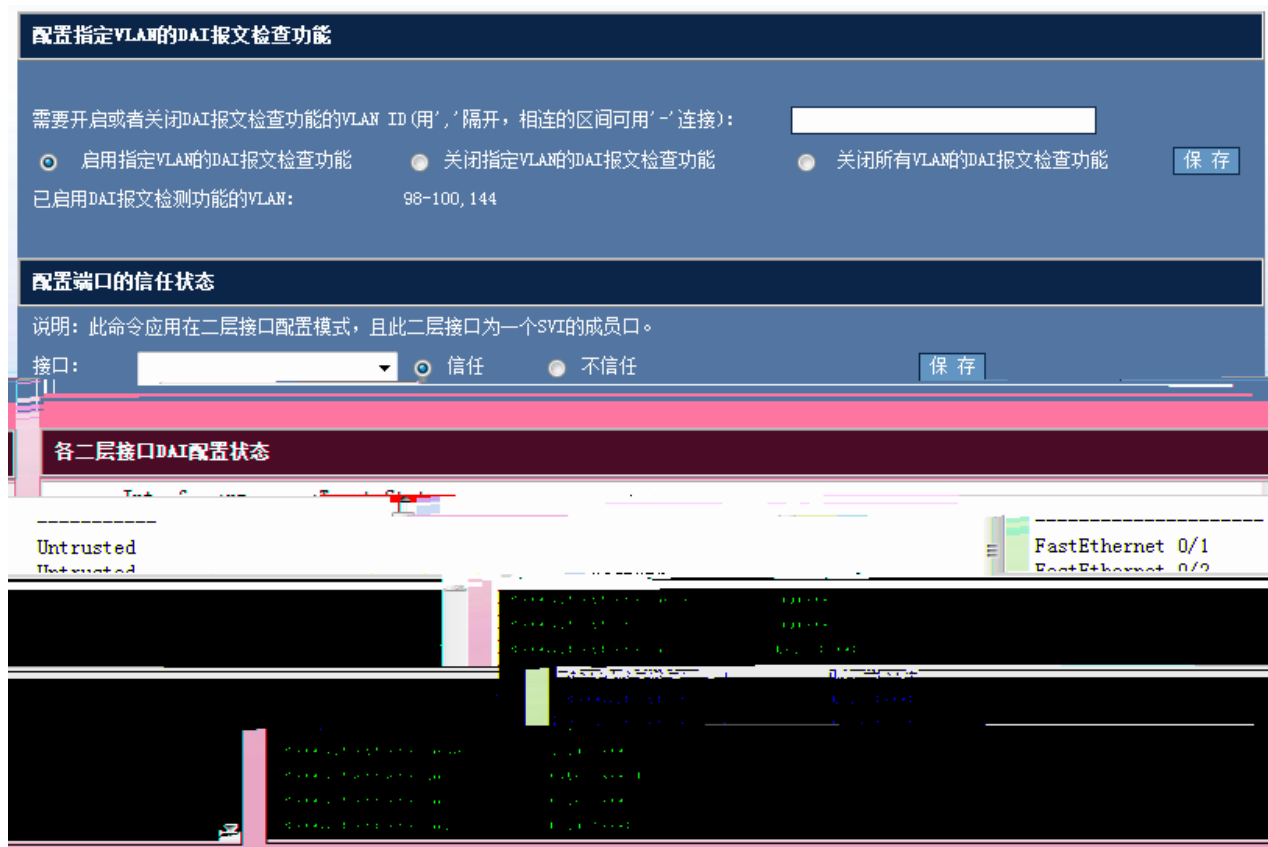
ARP

ARP

arp

“ DAI ”

DAI



45 DAI

1

VLAN	DAI
------	-----

VLAN DAI

VLAN 100 DAI

```
vlan-id    100    ARP          DAI
```

“

DAI

VLAN ID ”

VLAN

VLAN	DAI
------	-----

VLAN DAI

DAI

VLAN

2

ARP

DAI

ARP

ARP

DAI

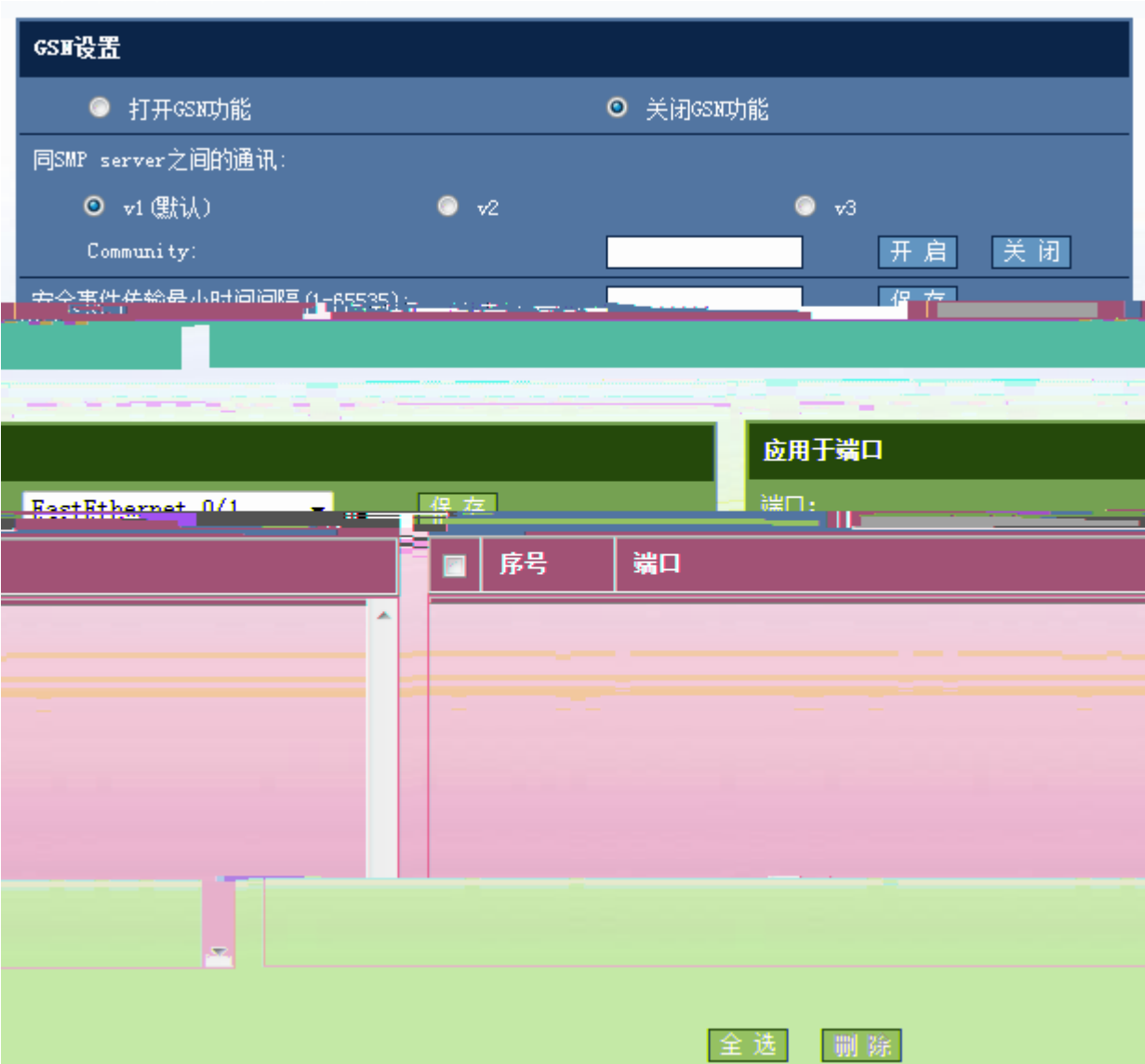
“ ” “ ”

“ DAI ”

2.3.7 GSN

“ GSN ”

GSN



46 GSN

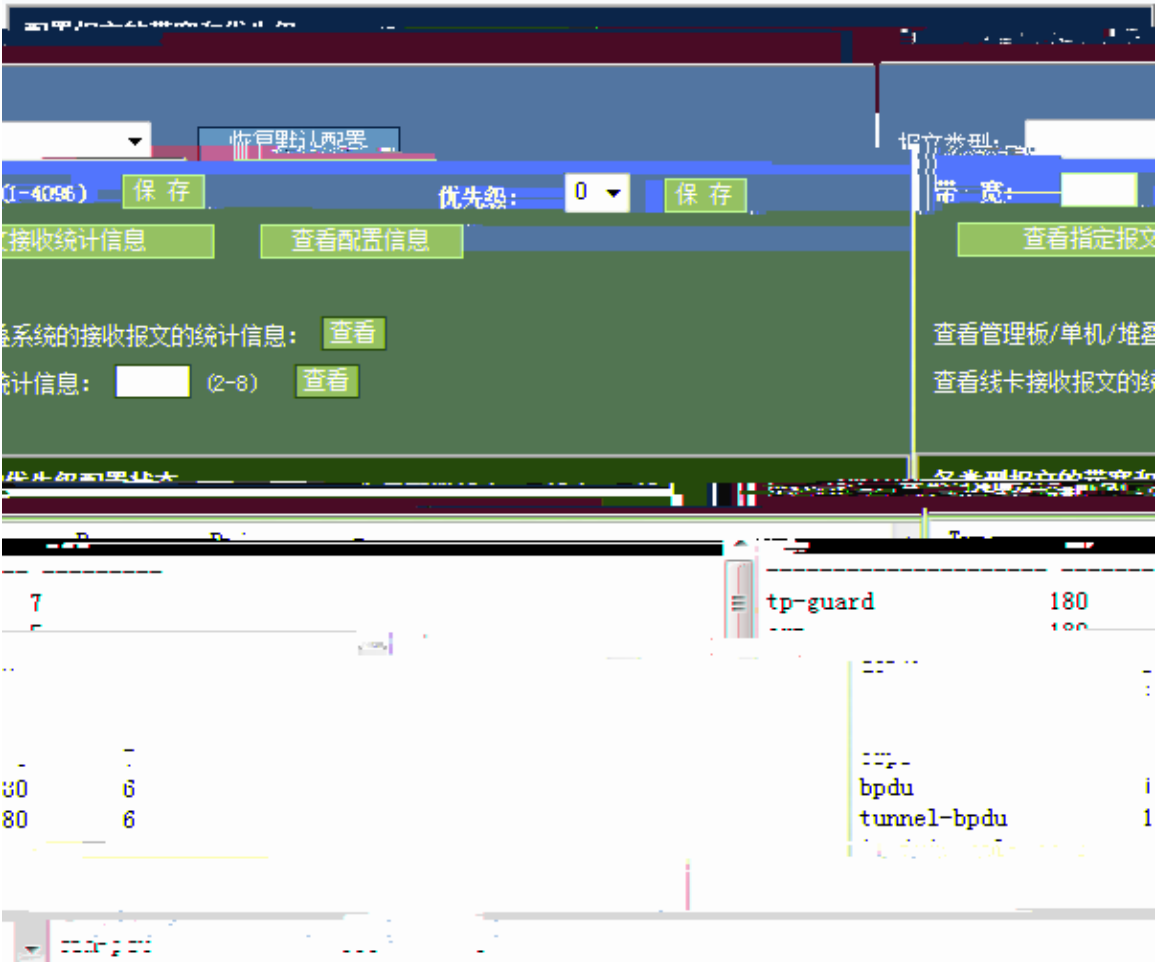
- 1) GSN
- GSN GSN GSN GSN
- 2) SMP server
- SMP server v1 v2 v3 Community
- User

3)

GSN GSN

2.3.8 CPP

“ CPP ”



47 CPP

“ ”

“ ”

“ ”

“ ”

arp报文接收统计信息				
Slot	Type	Pps	Total	Drop
MainBoard	arp	10	324430	0

48

“ ”

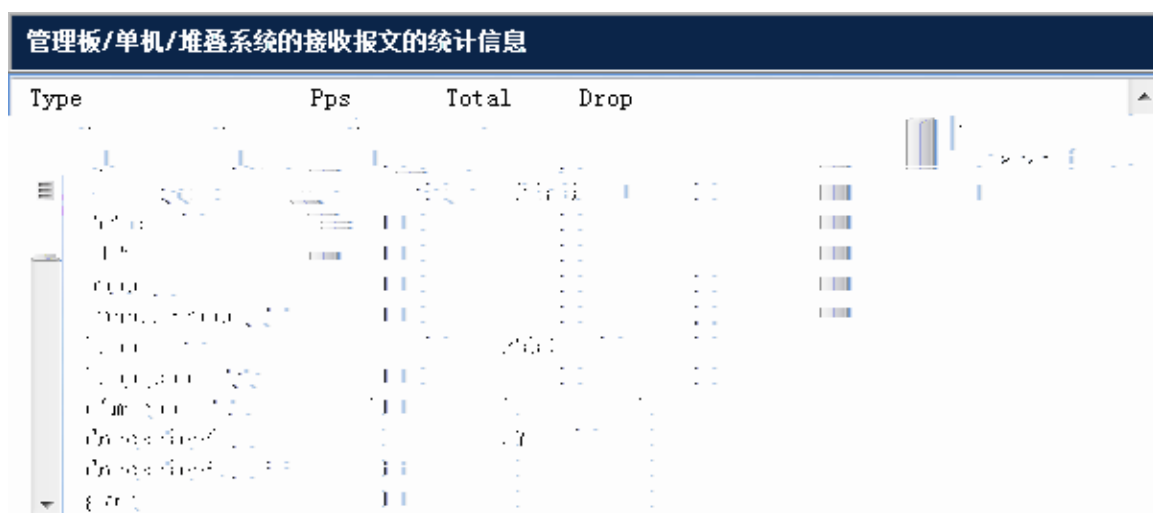
各类型报文的带宽和优先级配置状态				
Type	Pps	Pri		
tp-guard	180	7		
dot1x	2000	4		
rlldo	180	7		
	180	7		
	180	7		
	180	6		
tunnel-bpdu	180	6		
ipv4-icmp-local	1600	6		
lldp	180	5		
lldp_cdp	180	5		
cfm-pdu	180	3		

49

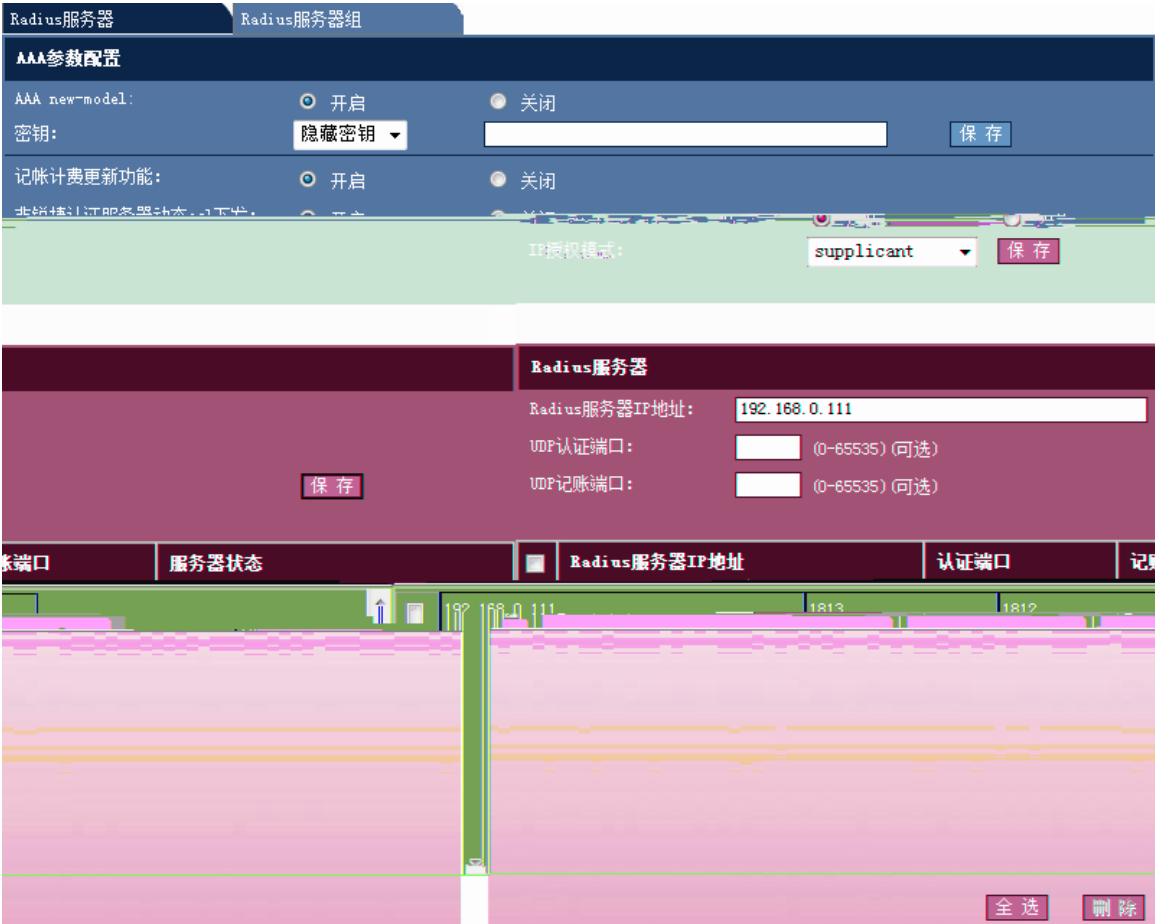
/ /

“ ”

/ /



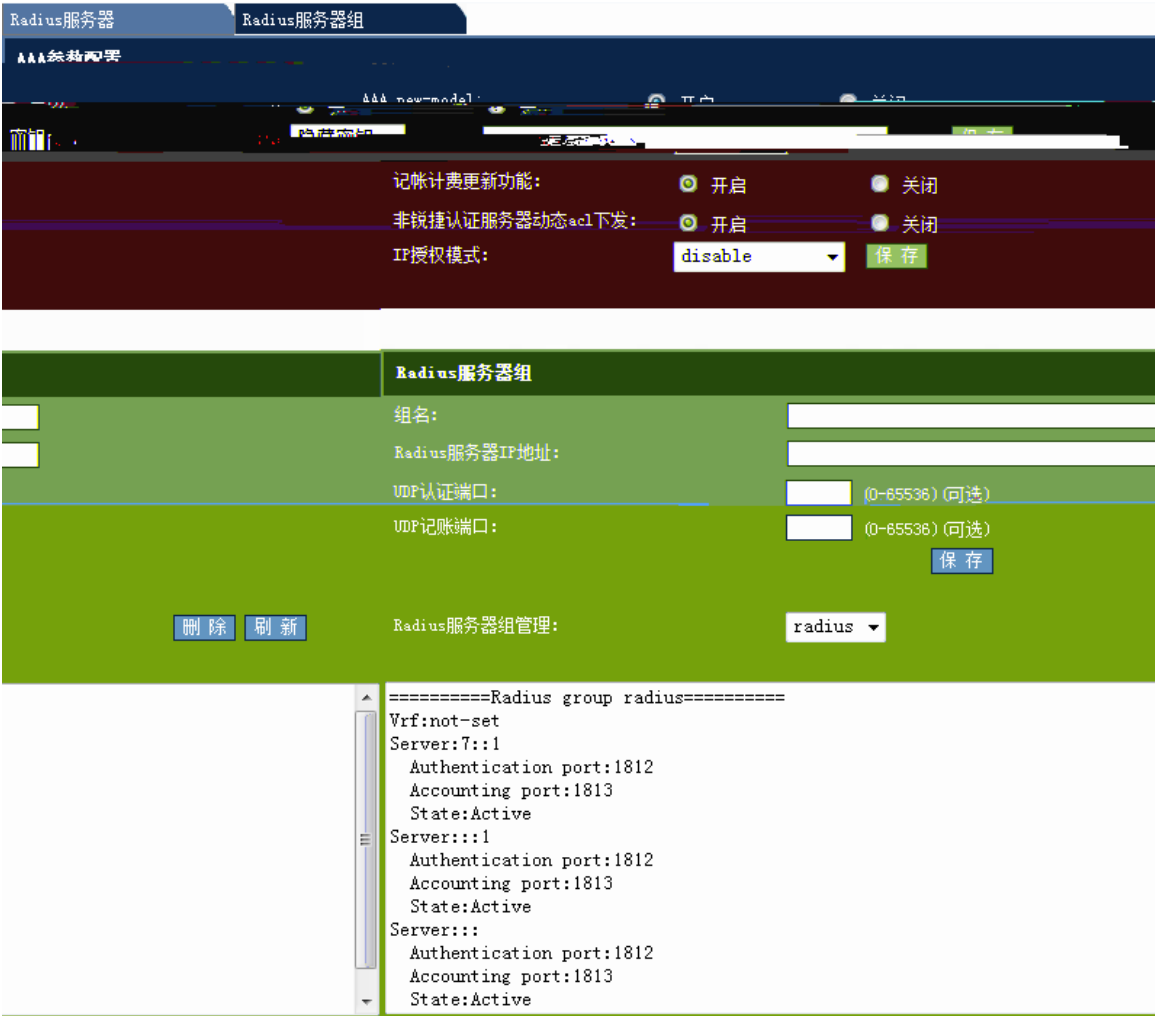
50 / /



51 RADIUS

AAA
AAA new-model
“ ”
IP
”
RADIUS
“ ”
AAA
“ ”
RADIUS
IP
“ ”

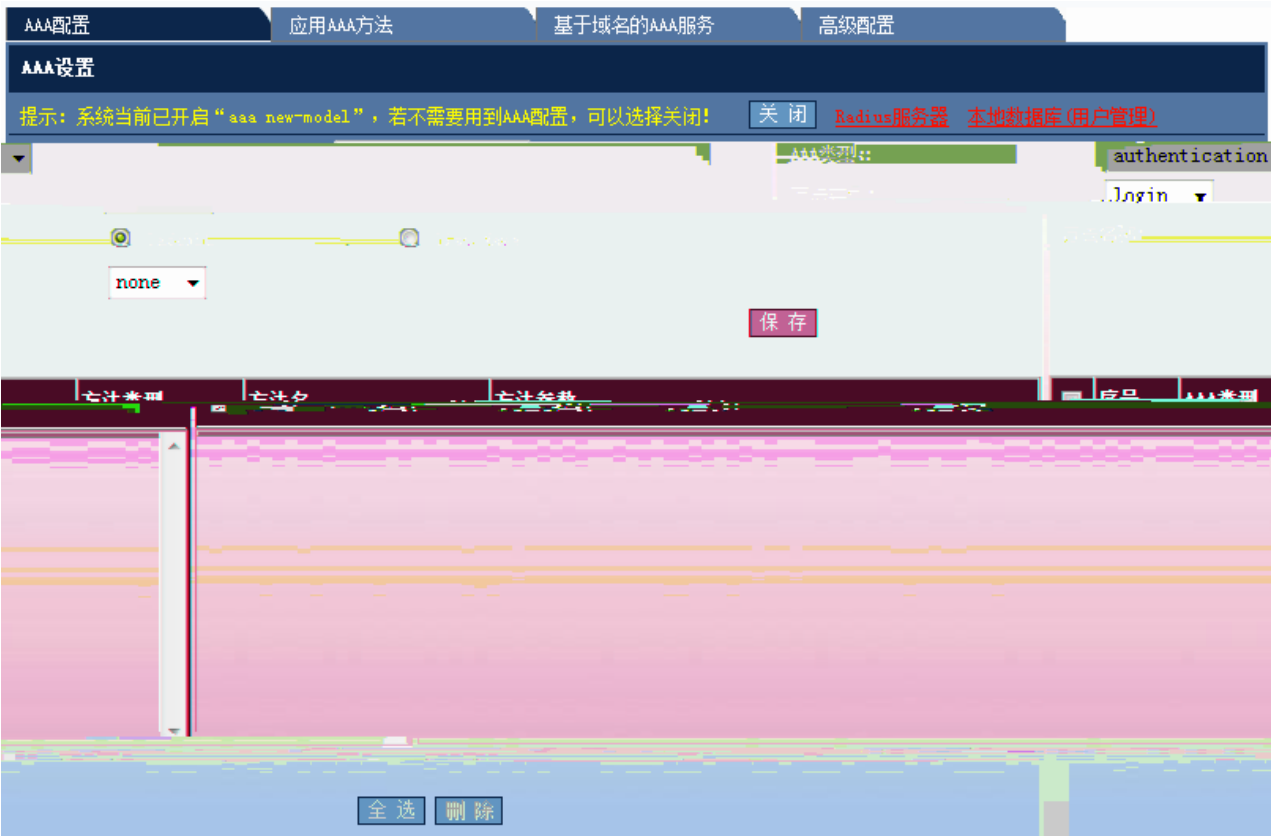
2 RADIUS



52 RADIUS

RADIUS IP

“ ”



53 AAA

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



54 AAA

AAA

AAA

3

AAA

AAA配置 应用AAA方法 基于域名的AAA服务 高级配置

基于域名的AAA服务

基于域名的AAA服务

域名: ☐ Default ☐ Domain Name

认证方法: default

授权方法: default

计费方法 (accounting): default

default

☒ With Domain ☐ Without Domain

Access Limit: 2

保存

删除

```

#default=====
#domain
#ic: 0

default
#default
# default
  
```

记账方法 (accounting):

用户名: 用户名是带域名的格式:

Access Limit (1-1024):

AAA Domain管理:

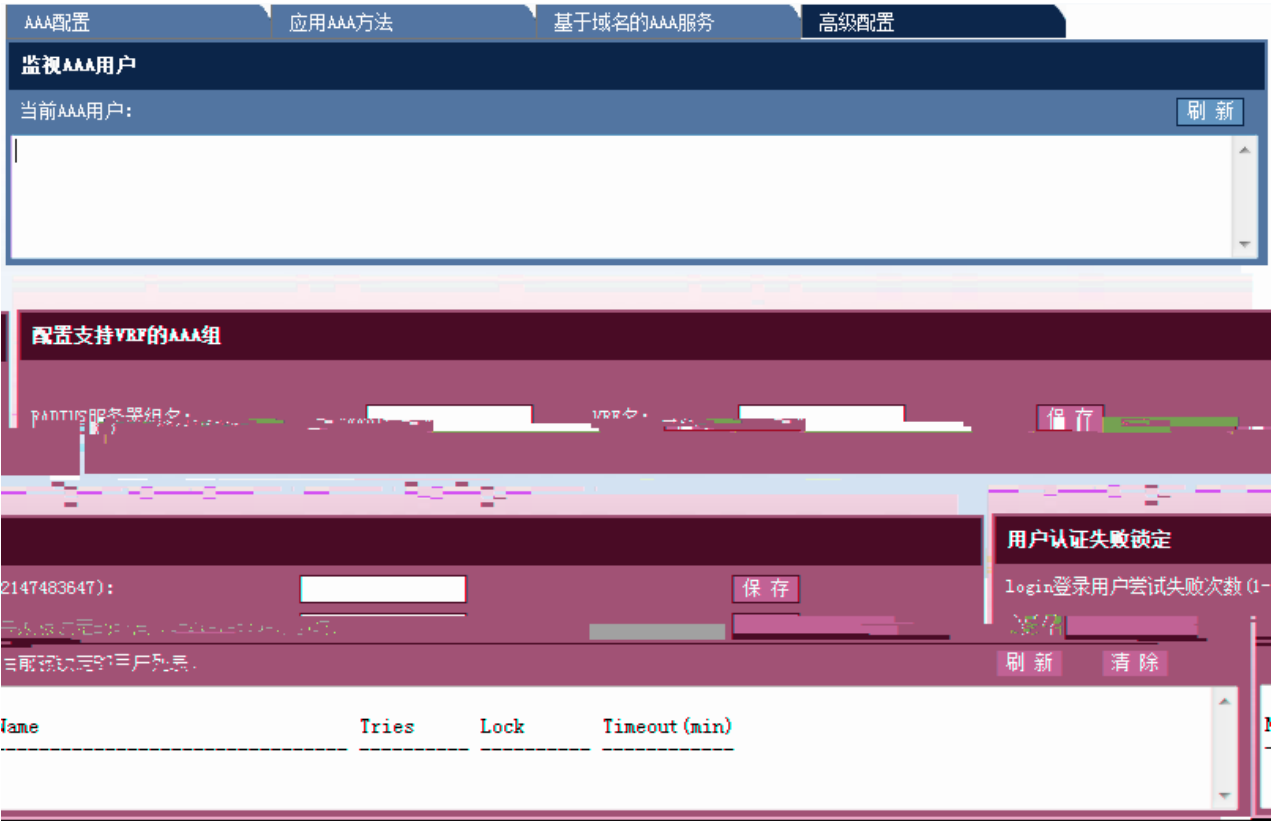
```

=====Domain d
State: Block
Username format: With
Access limit: 2
802.1X Access statist:

Selected method list:
authentication dot1x
authentication ppp d
authorization network
  
```

55

AAA

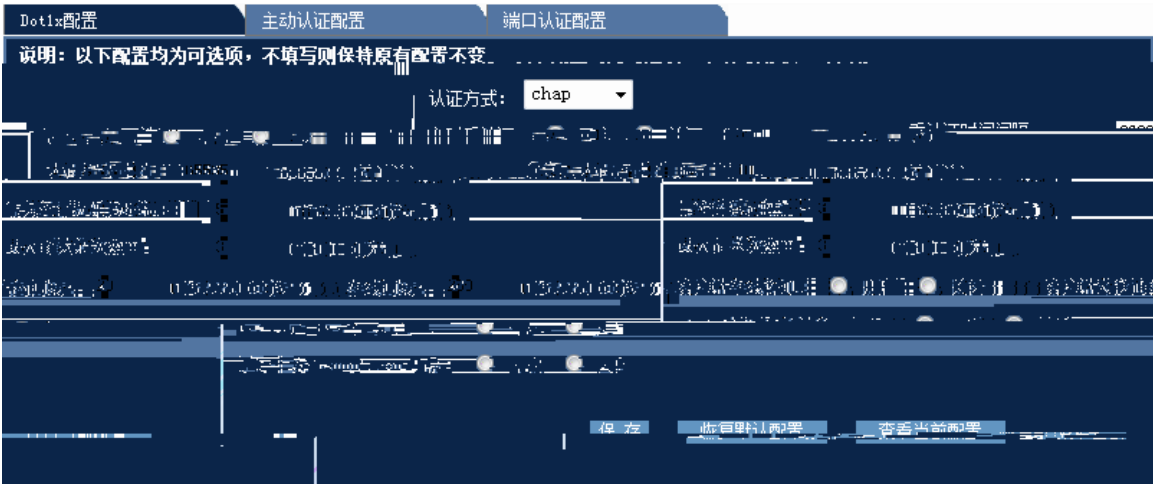


56 AAA
AAA AAA VRF AAA

2.3.11 Dot1x

“ Dot1x ”

1 Dot1x



57 Dot1x

Dot1x

2



58

3

Dot1x配置

主动认证配置

端口认证配置

说明：以下配置项均为可选。

端口：

FastEthernet 0/1

802.1x认证功能：

开启关闭

VLAN自动跳转功能：

开启关闭

Guest VLAN跳转：

开启关闭

Vlan Id： (1-4094)

端口的控制模式：

基于用户MAC

基于端口单用户的控制模式

MAC旁路认证：

开启关闭

MAC旁路认证超时时间： (1-65535)

MAC旁路认证违例：

开启关闭

保存

恢复默认

查看当前配置

禁止动态用户在多个认证端口之间迁移：

开启关闭 (默认值)

保存

端口下可认证主机列表

主机IP地址

端口

59

Dot1x

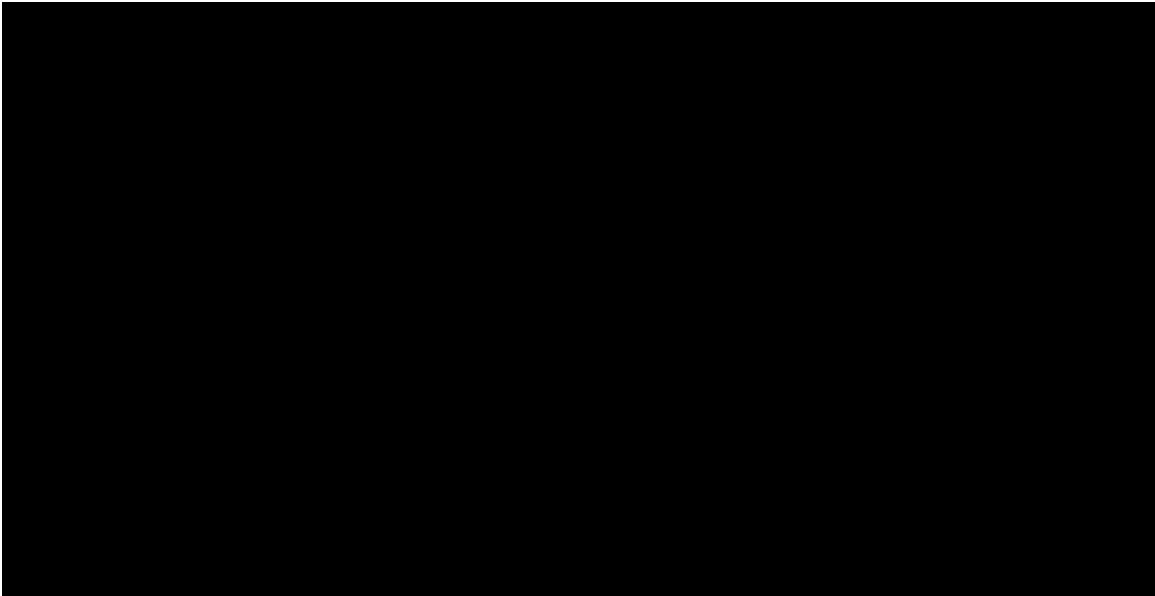
“ ”

“ ”

“

”

50



60

2

“ ”

802.1x



61

	IP	MAC		
1	IP		MAC	MAC
2	ARP	IP	MAC	

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	001e.ec0e.70ee	1	绑定
4	192.168.23.66	0023.ae86.b116	1	绑定
5	192.168.23.76	00d0.f886.66e0	1	绑定
6	192.168.23.83	0025.64af.cdee	1	绑定
7	192.168.23.93	0025.64c5.8970	1	绑定
8	192.168.23.94	0025.64c5.b2b9	1	绑定

刷新

62 ARP

2.3.13 WEB

“ web ”

web

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

重定向的IP地址:

0.0.0.0

认证页面URL:

重定向端口 (最多可以配置10个, 中间使用英文逗号分开):

80

未认证用户的最大HTTP会话数 (0-255, 可选):

255

每个端口下 (1-65535, 可选):

维持重定向连接的超时时间 (1-10秒, 可选):

3

保存

设备与认证服务器之间的通信密钥:

恢复默认

保存

保存

线用户信息的更新时间间隔 (30-3600秒):

60

恢复默认

提示: 多个Vlan之间使用英文逗号分开, 相连Vlan之间可以用“-”连接

63 web

- 1) web
- web

IP

URL

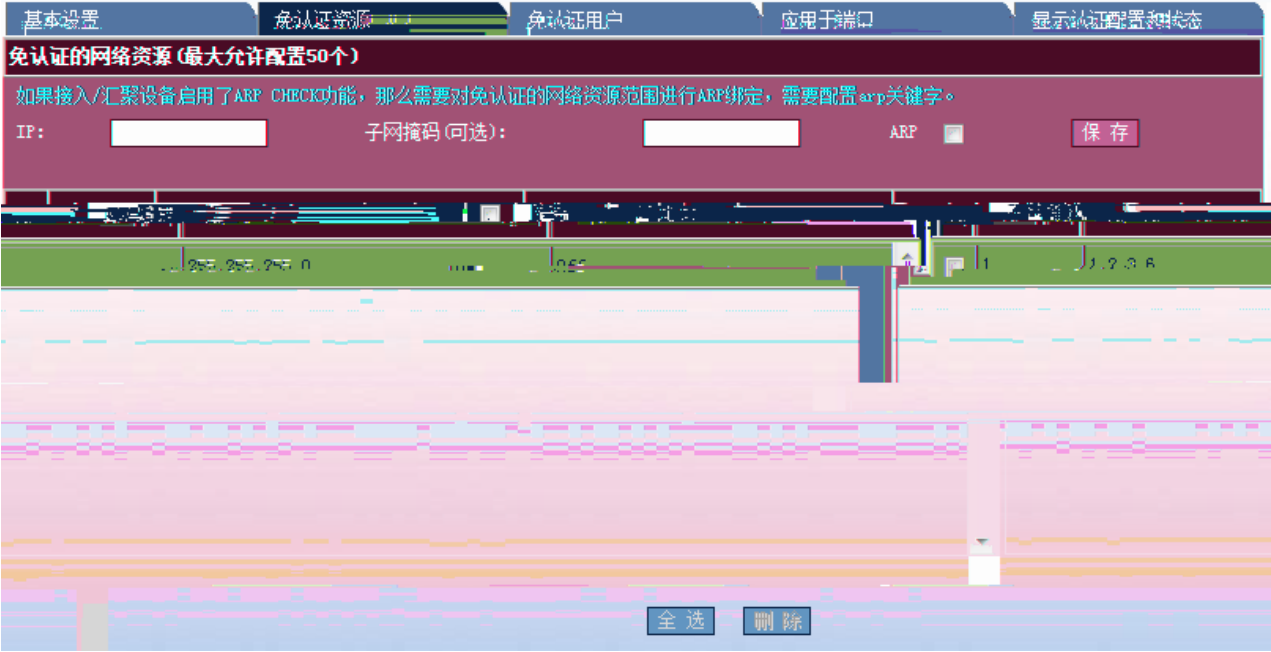
HTTP

(0-255)

Web

IP,SNMP-Inform

,Vlan List
- 2)



64

IP

3)



65

IP

4)

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

应用于端口

端口：

FastEthernet 0/3

IP Only Mode ☒

保存

☐	序号	端口	IP Only Mode
☐	1	FastEthernet 0/1	YES
☐	2	FastEthernet 0/3	YES

全选

删除

66

5)

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

查看所有用户的在线信息

0.0.0.0

查看指定用户的在线信息

67

2.3.14 DHCP Snooping

“ DHCP Snooping ”

DHCP Snooping

DHCP Snooping 设置

说明：DHCP Snooping就是DHCP窥探，通过对Client和服务端之间的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。

开启DHCP Snooping功能

关闭DHCP Snooping功能

开启DHCP源MAC检查功能

关闭DHCP源MAC检查功能

保存

DHCP Snooping 信任端口设置

添加信任端口

删除信任端口

批量删除信任端口

清除所有信任端口

端口：

FastEthernet 0/1

▼

保存

限速

信任端口

配置信息

端口

信任端口

68 DHCP Snooping

1)DHCP Snooping

DHCP Snooping DHCP Snooping MAC
“ ”

2)DHCP Snooping

“ ”
“ ”

2.4 QOS

2.4.1

“ ”

分类设置

说明：分类设置采用ACL的匹配规则识别出符合某类特征的数据流，并对该数据流进行标记。

类名：

ACL列表：

(ACL设置)

保存

■

类名

ACL

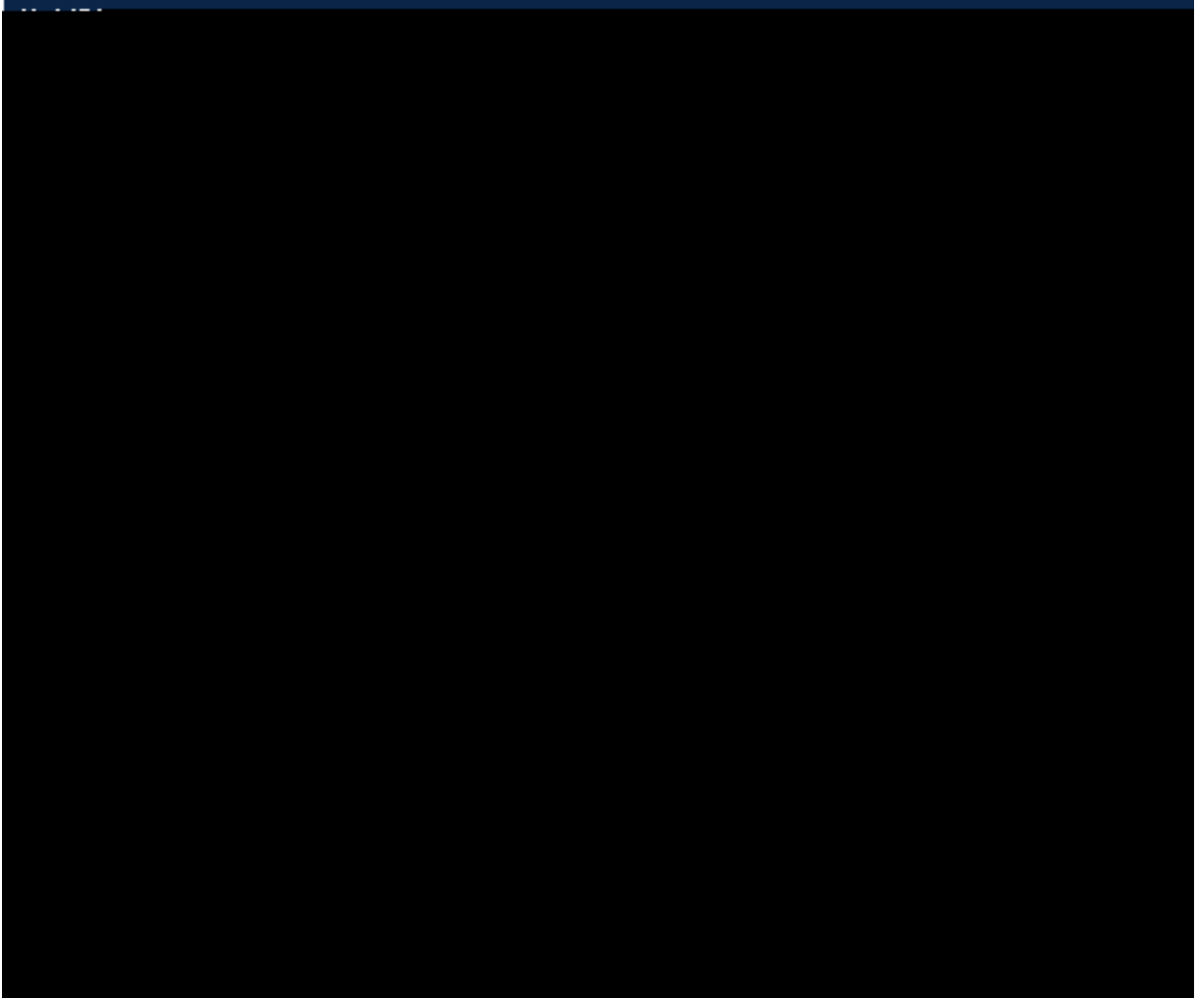
全选

删除

ACL “ ”
“ ”

2.4.2

“ ”



70

“ ”

“ ”

2.4.3

“ ”

流设置

说明：应用策略设置对端口的输入或输出流进行限制。

端 口：

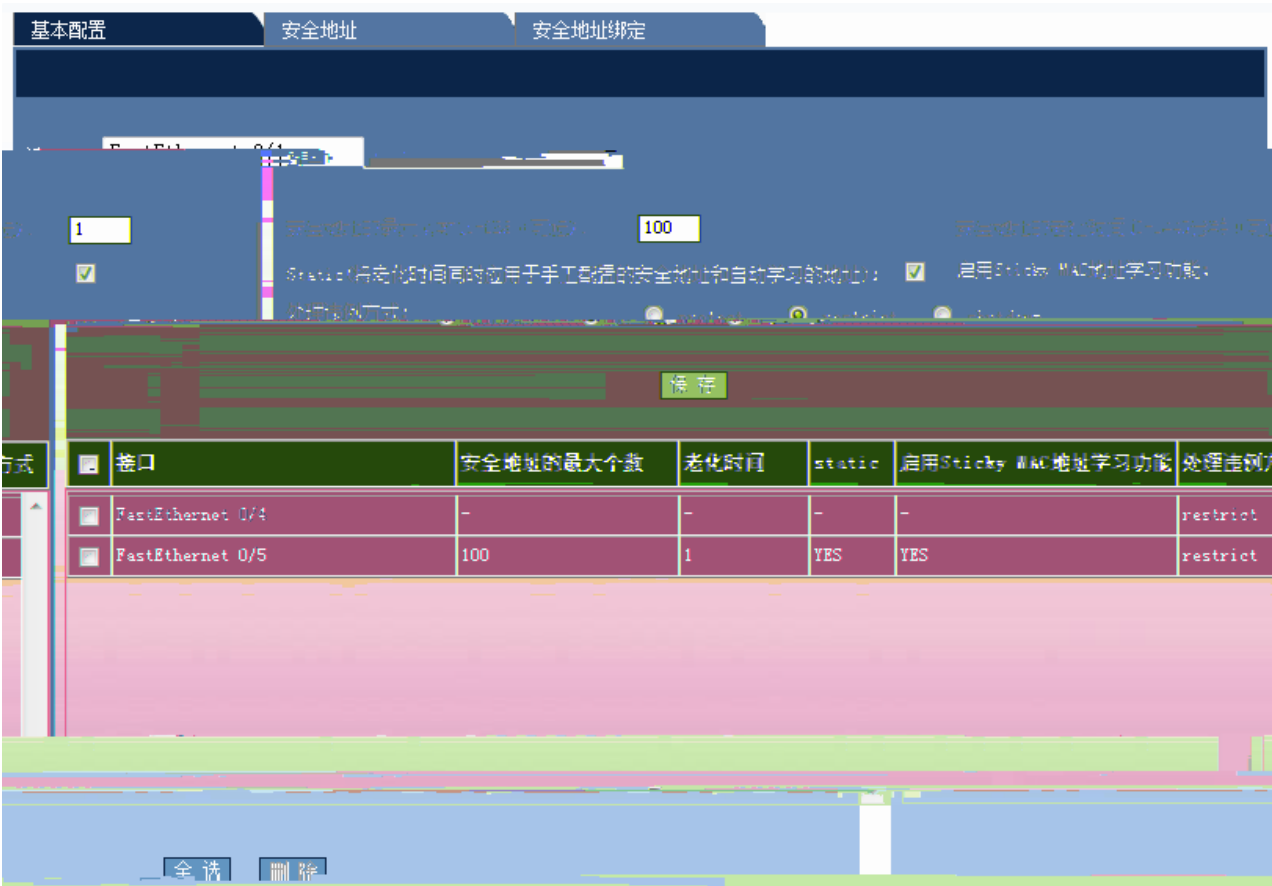
策略列表： [\(策略设置\)](#)

限速方向： ☒ 输入限速 ☐ 输出限速

☐	端口	方向	策略名	信任模式	COS
☐	FastEthernet 0/1	-	-	-	-
☐	FastEthernet 0/2	-	-	-	-
☐	FastEthernet 0/3	-	-	-	-
☐	FastEthernet 0/4	-	-	-	-
☐	FastEthernet 0/5	-	-	-	-
☐	FastEthernet 0/6	-	-	-	-
☐	FastEthernet 0/7	-	-	-	-
☐	FastEthernet 0/8	-	-	-	-
☐	FastEthernet 0/9	-	-	-	-
☐	FastEthernet 0/10	-	-	-	-
☐	FastEthernet 0/11	-	-	-	-

“ ”
“ ”

2.4.4



73

1)

Sticky Mac

Static

“ ”

2)

基本配置

安全地址

安全地址绑定

端口: FastEthernet 0/1

MAC地址: 1000.0000.0003

Vlan ID: 2

保存

接口	类型	MAC地址	Vlan ID
☒ FastEthernet 0/3	-	1000.0000.0000	2
☒ FastEthernet 0/5	sticky	1000.0000.0003	2

全选

删除

74

Mac VLAN ID

3)

基本配置

安全地址

安全地址绑定

端口：

FastEthernet 0/1

IP地址 (IPv4或IPv6):

1.2.3.3

将MAC及Vlan进行绑定到安全端口：

☒

MAC地址：

1000.0000.0000

Vlan ID：

10

保存

☐	接口	MAC地址	Vlan ID	IP地址
☐	1000	10	1.2.3.3	☐ FastEthernet 0/1 1000.0000

全选

删除

75

Mac

IP
VLAN ID

MAC

Vlan

2.5

2.5.1

“ ”

系统信息	
设备型号：	S2924G
主机名：	Ruijie
设备版本：	00555 : Ruijie's Embedded Software Version 7.0.0.10000
设备名称：	SW17
MAC地址：	001000000000

76

2.5.2

“ ”

```
Building configuration...
Current configuration : 12931 bytes
!
version RGNOS 10.2.00(3), Release(30355) (Tue Mar 11 19:23:04 2008 - 23195A44470348C)
!
!
!
vlan 1
 name vlan1
!
vlan 2
!
vlan 3
!
vlan 4
!
vlan 5
!
vlan 6
!
vlan 7
!
```

77

2.5.3

“ ”

端口状态					
端 口	状 态	Vlan	双 工	速 率	端口类型
FastEthernet 0/1	down	1	Unknown	Unknown	copper
FastEthernet 0/2	down	2	Unknown	Unknown	copper
FastEthernet 0/3	up	1	Full	100M	copper
FastEthernet 0/4	down	900	Unknown	Unknown	copper
FastEthernet 0/5	down	1	Unknown	Unknown	copper
FastEthernet 0/6	down	1	Unknown	Unknown	copper
FastEthernet 0/7	down	1	Unknown	Unknown	copper
FastEthernet 0/8	down	1	Unknown	Unknown	copper
FastEthernet 0/9	down	1	Unknown	Unknown	copper
FastEthernet 0/10	down	1	Unknown	Unknown	copper

刷新

78

2.5.4

“ ”

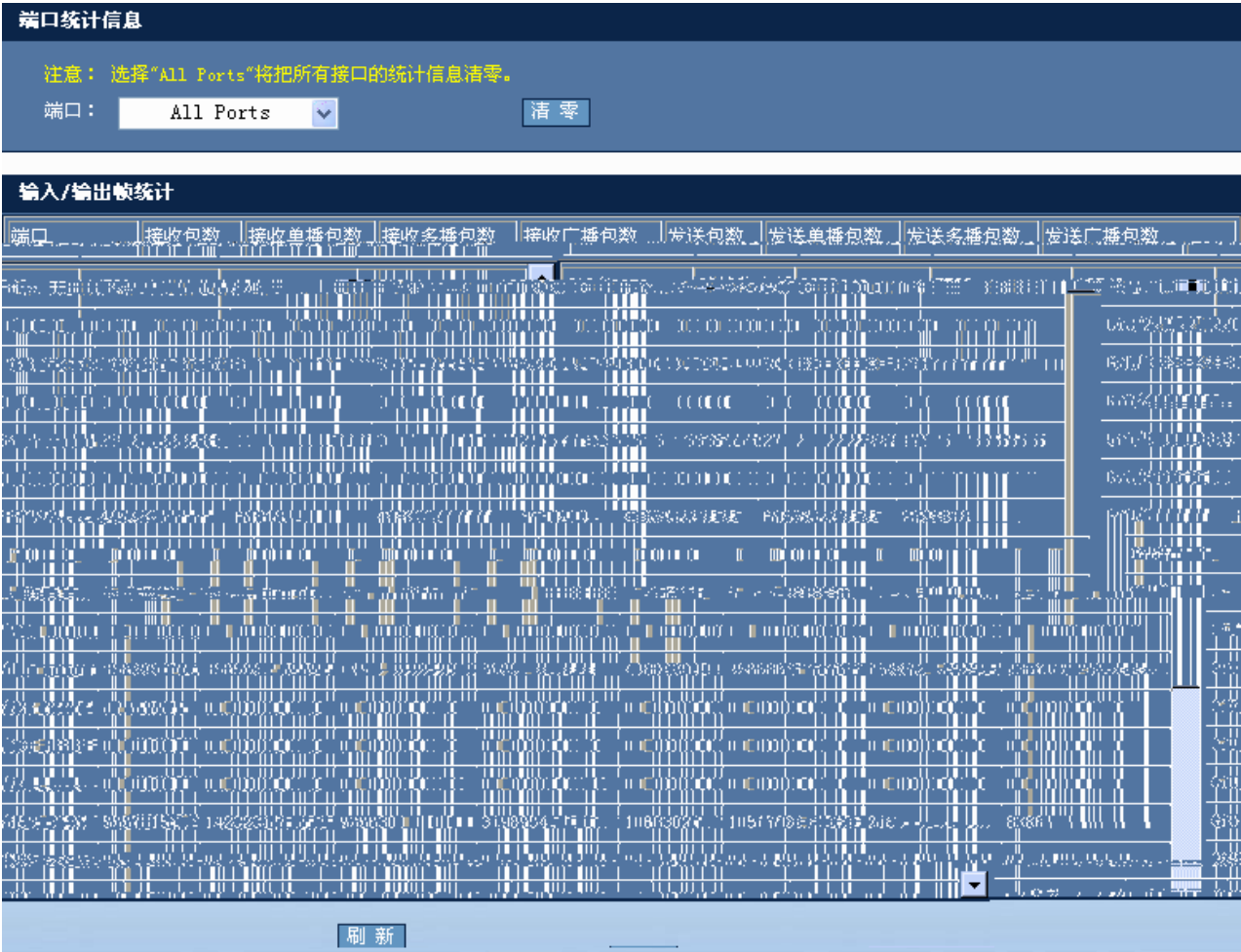
端口运行状态	
端 口	带宽占用
FastEthernet 0/1	0%
FastEthernet 0/2	0%
FastEthernet 0/3	0%
FastEthernet 0/4	0%
FastEthernet 0/5	0%
FastEthernet 0/6	0%
FastEthernet 0/7	0%
FastEthernet 0/8	0%
FastEthernet 0/9	0%
FastEthernet 0/10	0%

刷新

79

2.5.5

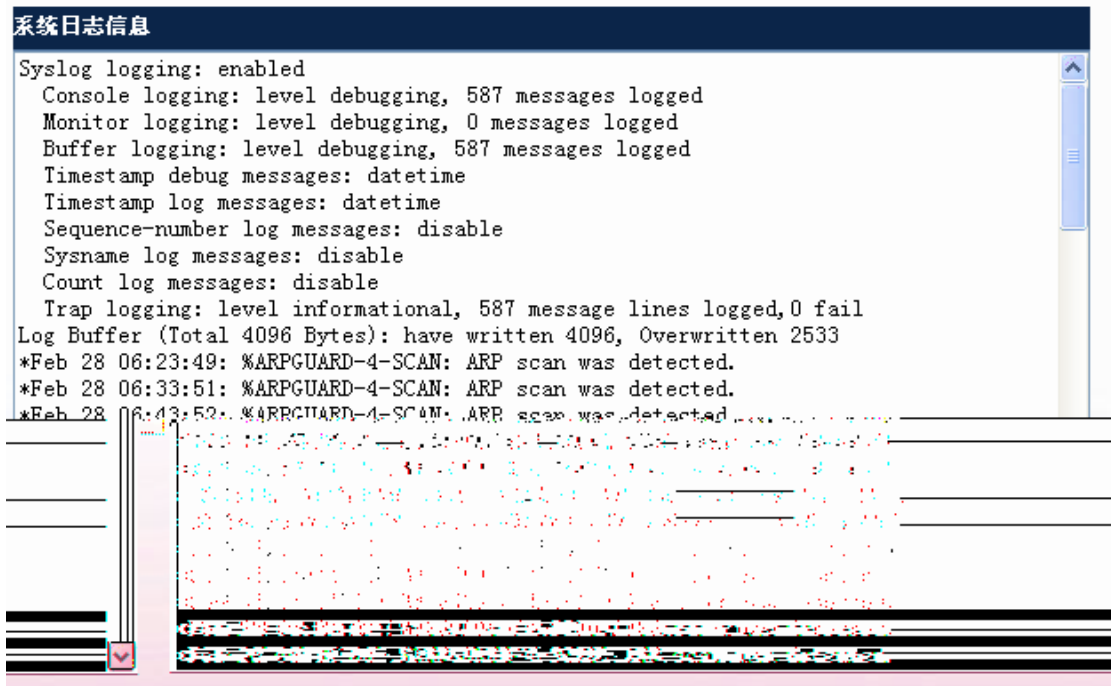
“ ”



80

2.5.6

“ ”



IP

“

”

IP

Ping

2.6.2 Telnet

Test EE`
Telnet`

用户管理		
☐	序号	用户名
☐	1	admin

84

“ ”

用户管理 -- 网页对话框

用户名 :

用户密码 :

密码确认 :

保存

取消

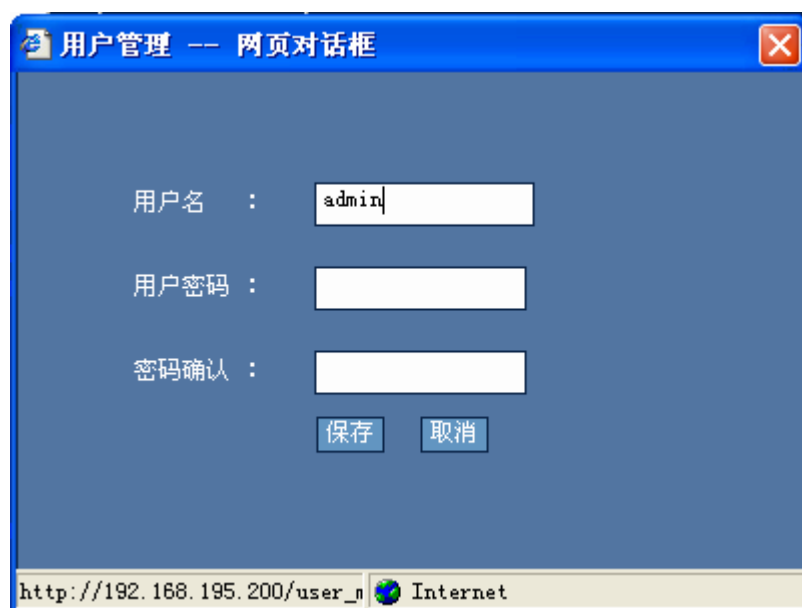
http://192.168.195.200/user_m Internet

85

“ ”

“ ”

“ ”



用户管理 -- 网页对话框

用户名 : admin

用户密码 :

密码确认 :

保存 取消

http://192.168.195.200/user_m Internet

86

“ ”



2.6.5 /

“ / ”

/

导入/导出配置

注意：请确认TFTP服务器已启用！

TFTP服务器 IP :

TFTP服务器 文件名 :

文件传输信息：

89 /

config.text TFTP IP TFTP

“ ”

2.6.6 WEB

“ WEB ”

WEB

WEB端口设置

注意：修改WEB端口后，请用新端口重新登录。如果要使用80端口，请直接单击“使用默认端口按钮”。

指定WEB端口： (1025-65535)

90 WEB

“ ”

8080 IP 192.168.1.1

<http://192.168.1.1:8080> “ ”
<http://192.168.1.1>

2.6.7

“ ”



91

TFTP TFTP
TFTP IP “ ”

2.6.8

“ ”

“ ”

2.7

2.8 WEB

2.8.1

2.8.2

2.8.3

WEB	WEB	enable
-----	-----	--------

2.8.4

WEB	Local	Enable
WEB		WEB

1 Local

a. config

Ruijie#configure

Enter configuration commands, one per line. End with CNTL/Z.

b. WEB

Ruijie(config)#enable service web-server

c. WEB Local

Ruijie(config)#ip http authentication local

d. 15

Ruijie(config)#username admin password admin

Ruijie(config)#username admin privilege 15

e. IP

```
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 192.168.100.1 255.255.255.0
2    Enable
```

a. config

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
```

b. WEB

```
Ruijie(config)#enable service web-server
```

c. WEB Enable

```
Ruijie(config)#ip http authentication enable
```

d. Enable

```
Ruijie(config)#enable password admin
```

e. IP

```
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 192.168.100.1 255.255.255.0
```

2.8.5

1 Local

```
Ruijie(config)#show running-config
Building configuration...
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
    ip address 192.168.100.1 255.255.255.0 // IP
    no shutdown
!
!
line con 0
line vty 0 4
    login
!
!
end
```

2 Enable

Ruijie(config)#show running-config

Building configuration...

Current configuration : 2014 bytes

```
!
version RGOS 10.2(4), Release(55435)(Wed May 13 11:50:07 CST 2009
-ngcf32)
vlan 1

no service password-encryption
!
enable password admin //WEB Enable
enable service web-server // WEB
!
....
.....
!
interface VLAN 1
    ip address 192.168.100.1 255.255.255.0 // IP
    no shutdown
!
!
```

```
line con 0
line vty 0 4
  login
  !
  !
end
```

