



**WEB**

**RG-S5750-@**

**RGOS 10.4(2b12)p1**

**V1.0**

©2000-2013



■ <http://www.ruijie.com.cn/>

■ <http://webchat.ruijie.com.cn>

8:30 6

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

■ 7 24 4008-111-000

■ <http://support.ruijie.com.cn>

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

# RGOS<sup>®</sup>10.4 (2b12)p1

- 
- 
- 

## 1.

```
[ ]      [ ]  
{ x | y | ... }  
[ x | y | ... ]  
//
```

## 2.



3.

■

■

■



WEB

---

WEB

1. WEB

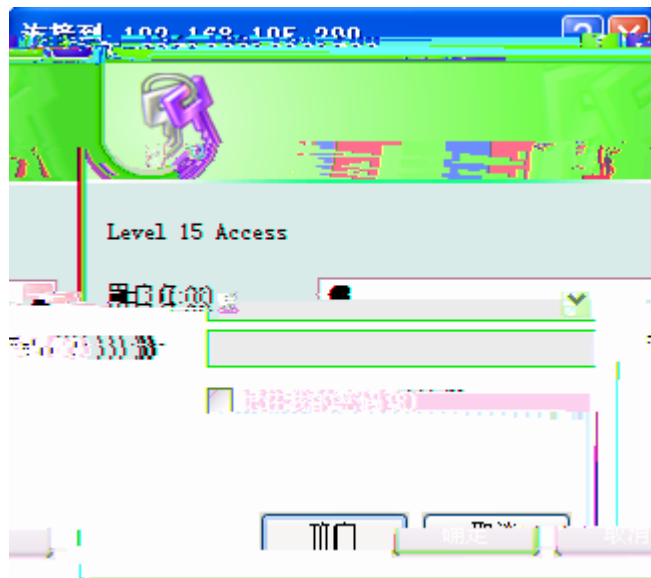
2. WEB

# 1 WEB

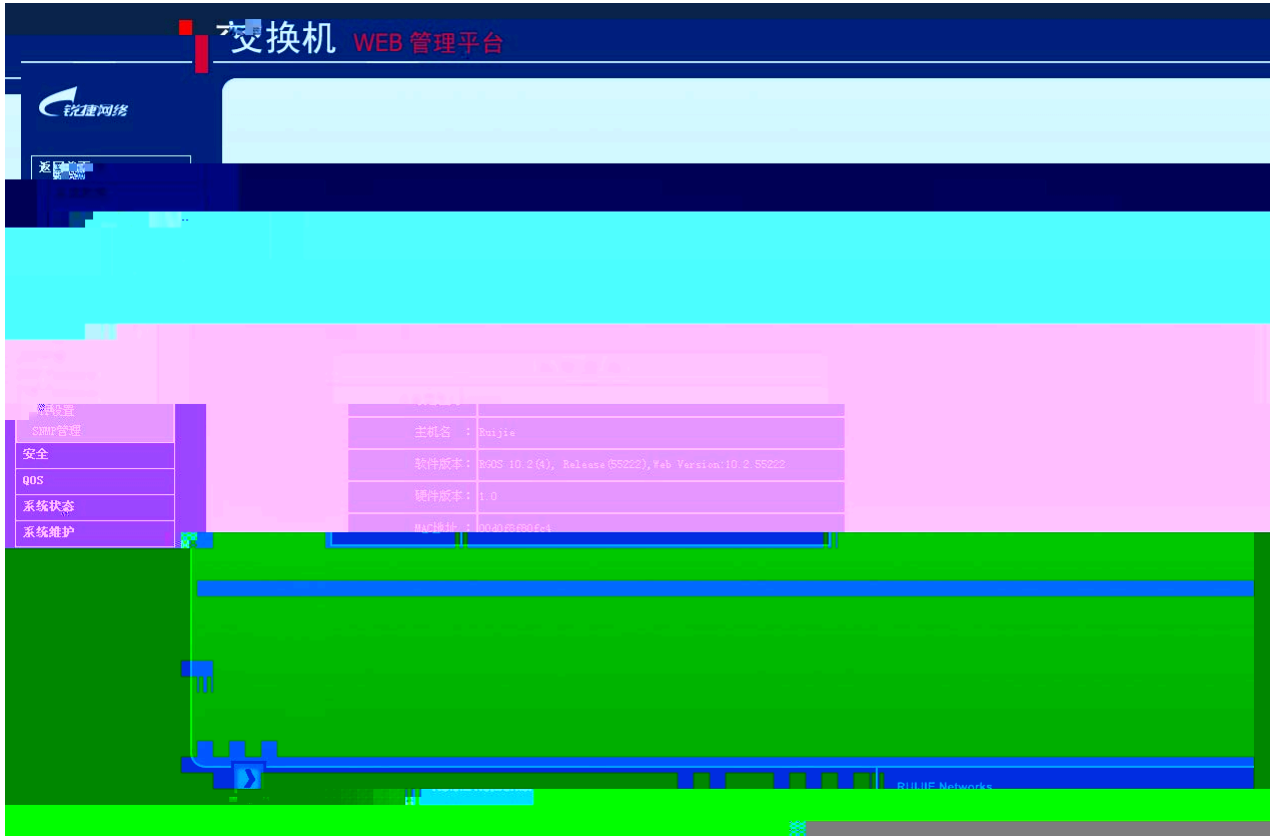
WEB



1



2



3 WEB

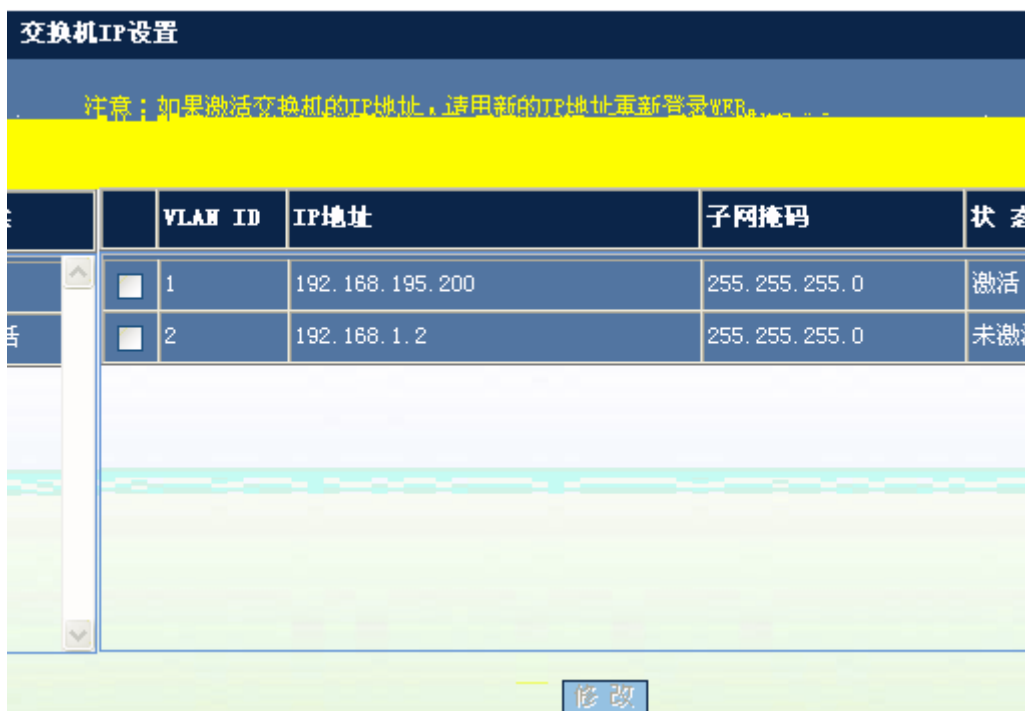
	WEB	Enable
	enable	

## 2.2

### 2.2.1 IP

IP

IP



4 IP

ip



5 IP

IP

## 2.2.2 VLAN

### VLAN

#### 1 VLAN

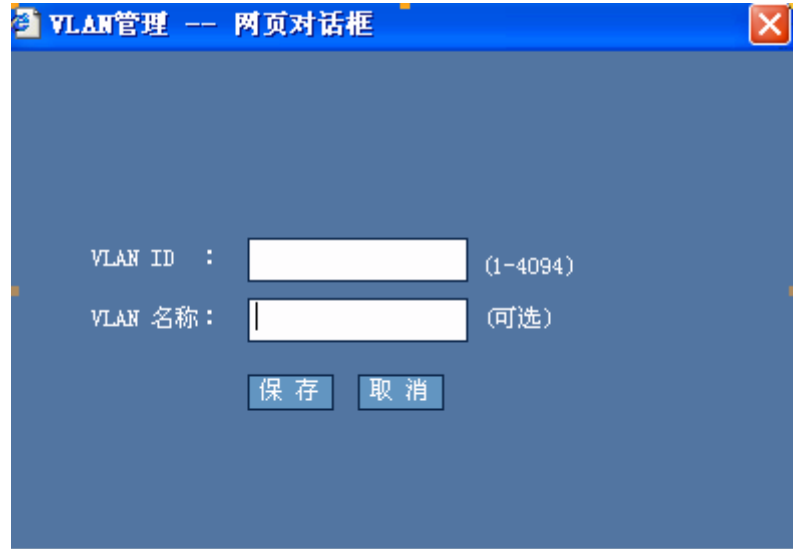


6 VLAN

VLAN

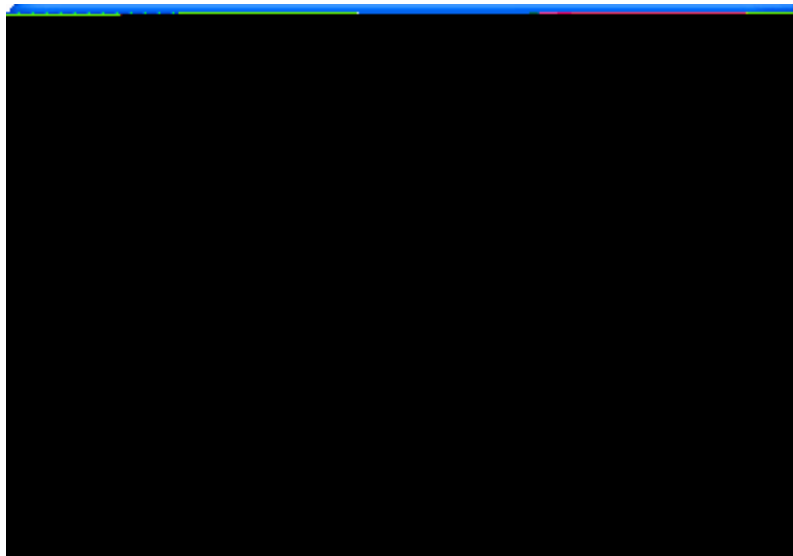
VLAN

VLAN



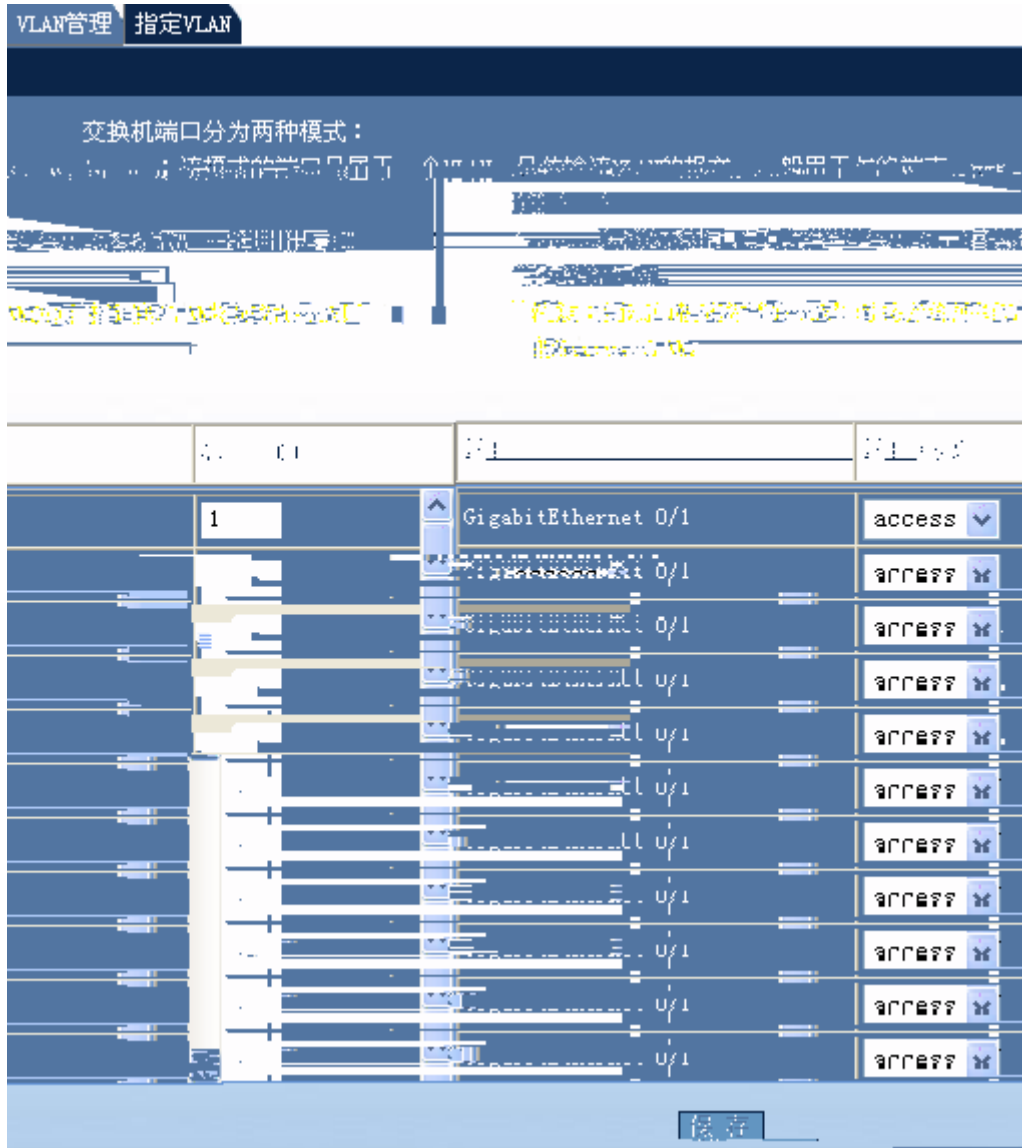
7 VLAN

VLAN ID VLAN  
VLAN VLAN  
VLAN  
VLAN



8 VLAN

VLAN  
VLAN  
2 VLAN

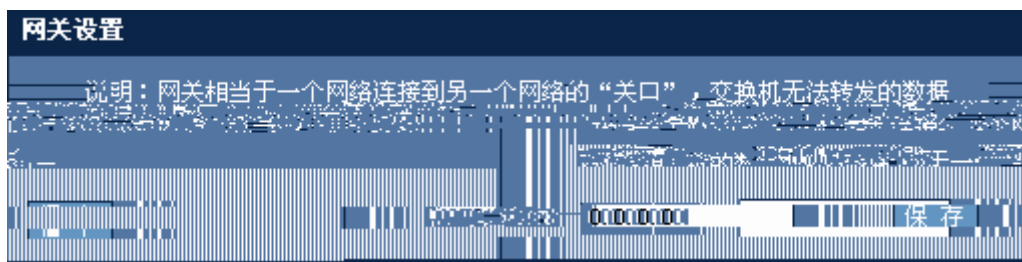


9 VLAN

VLAN ID

2.2.3

配置VLAN



10

IP

IP

## 2.2.4



11

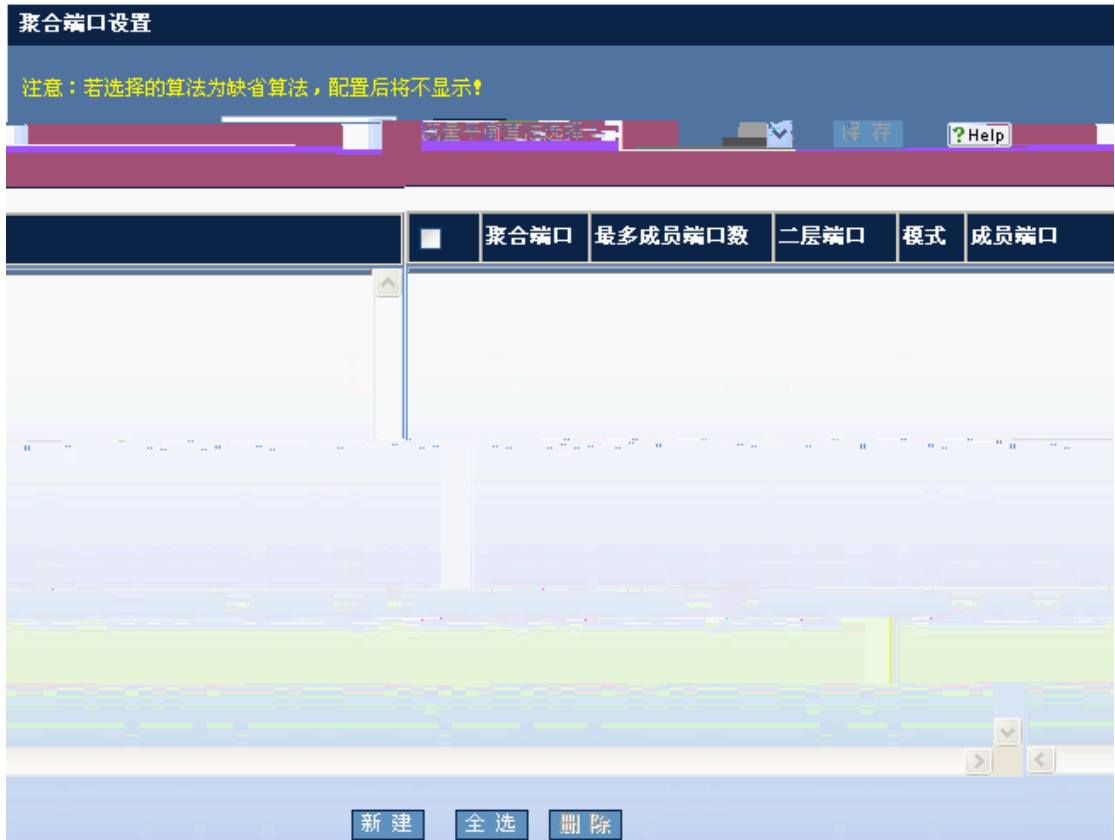
## 2.2.5

**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	<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"/>
GigabitEthernet 0/12	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/13	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/14	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/15	<input type="text"/>	<input type="text"/>

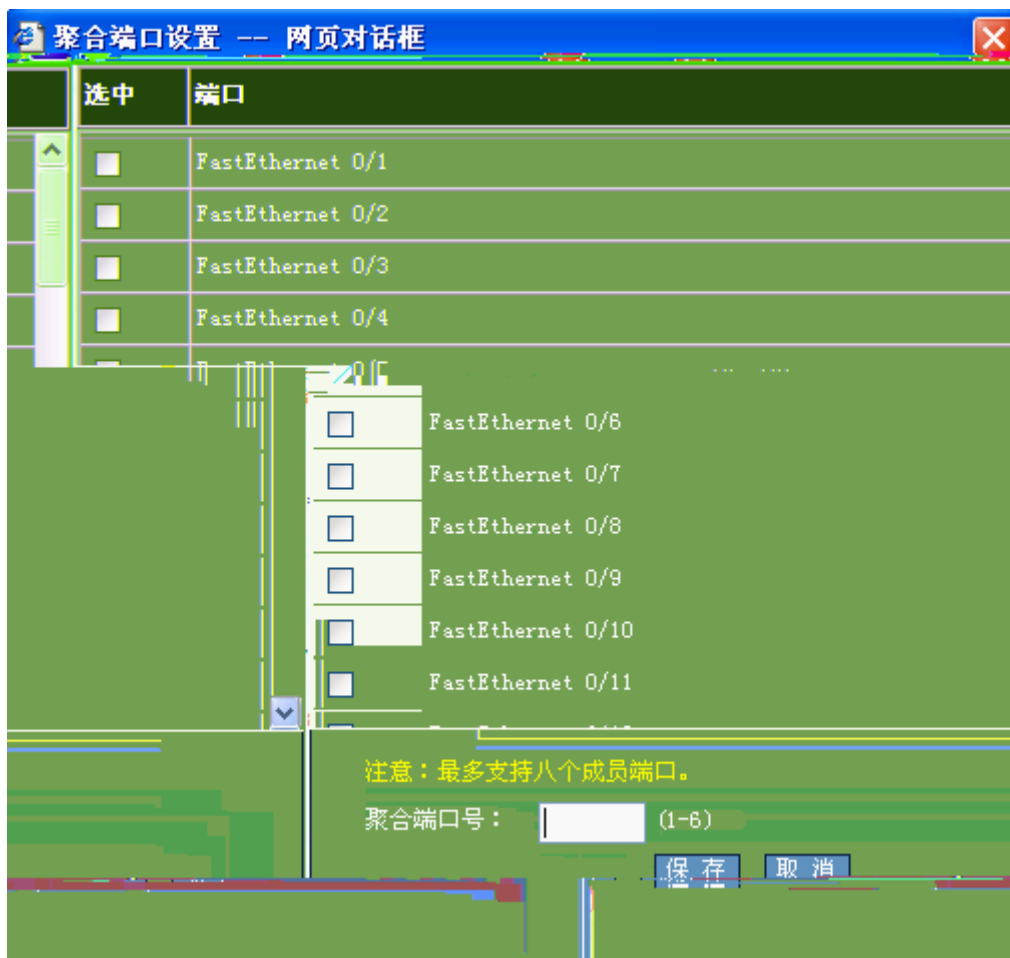
### 2.2.6



13

1

2





### 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：  保存

### DHCP服务器

操作	IP地址	网段	状态
全选			
删除			

16 DHCP

1) / DHCP

/ DHCP

2)DHCP

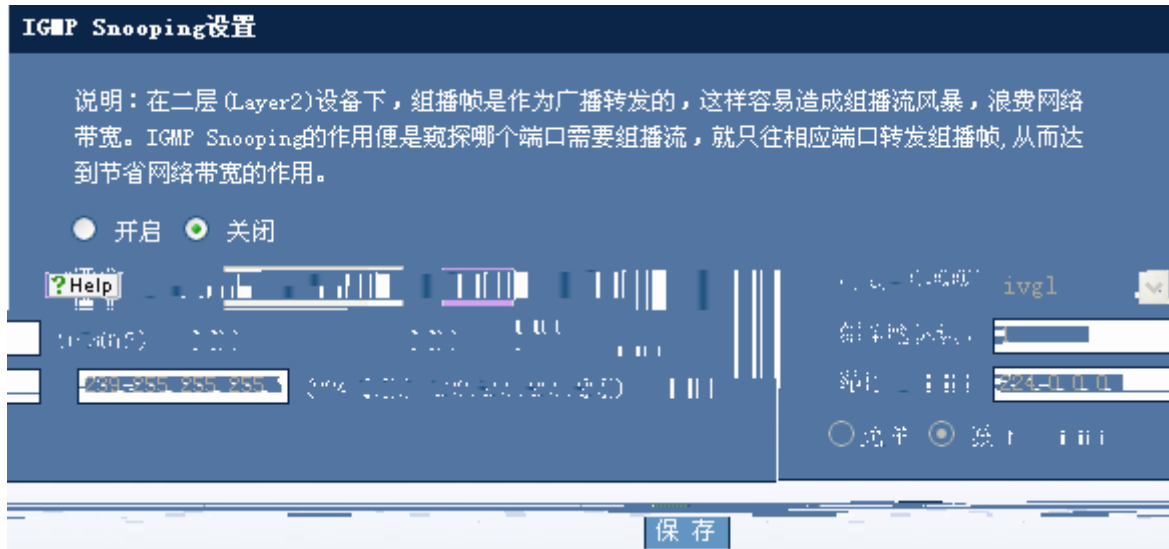
DHCP

DHCP

## 2.2.9 IGMP Snooping

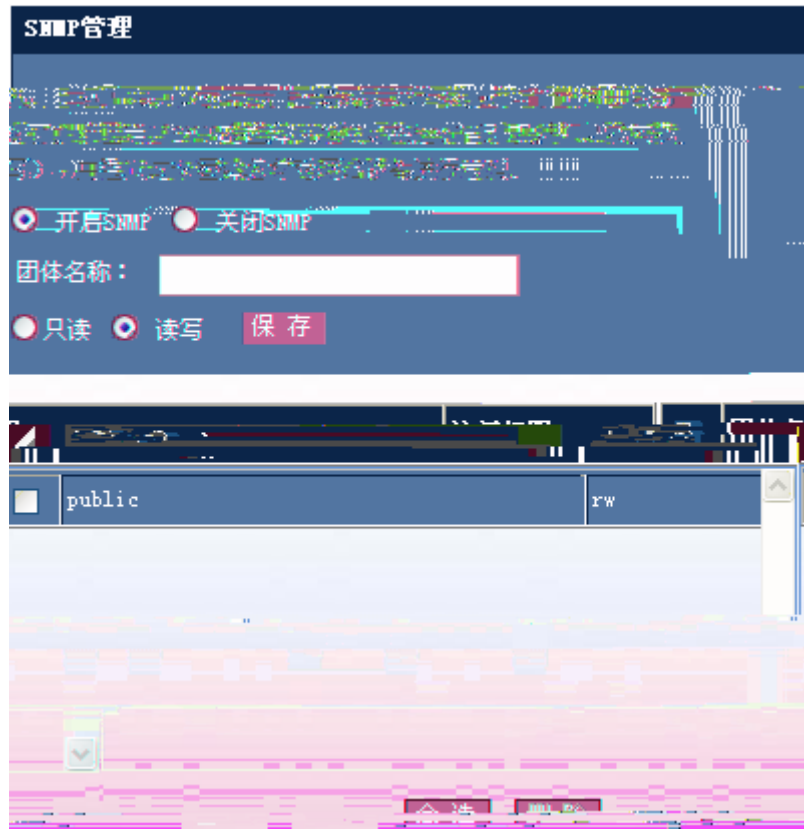
IGMP Snooping

IGMP Snooping



1 A m

## SNMP



19 SNMP

SNMP

SNMP

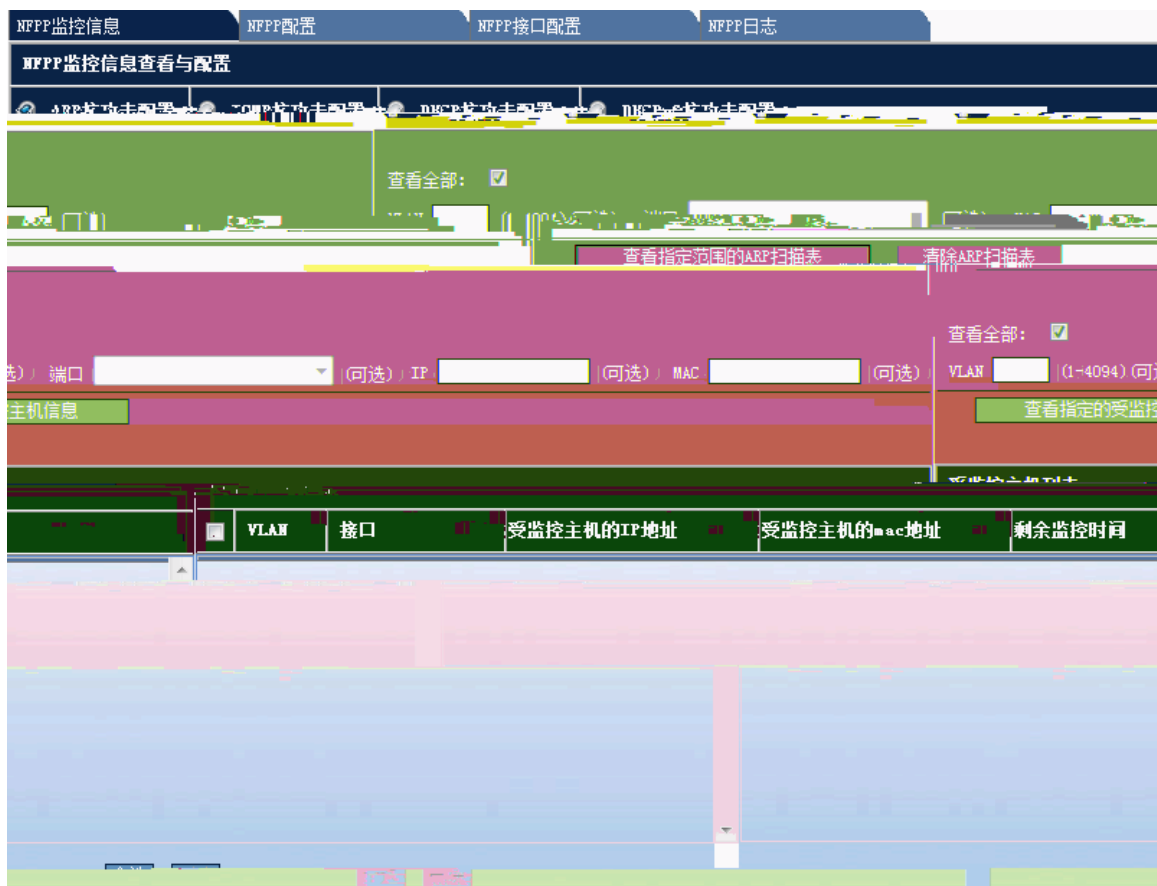
SNMP

SNMP

## 2.2.12 NFPP

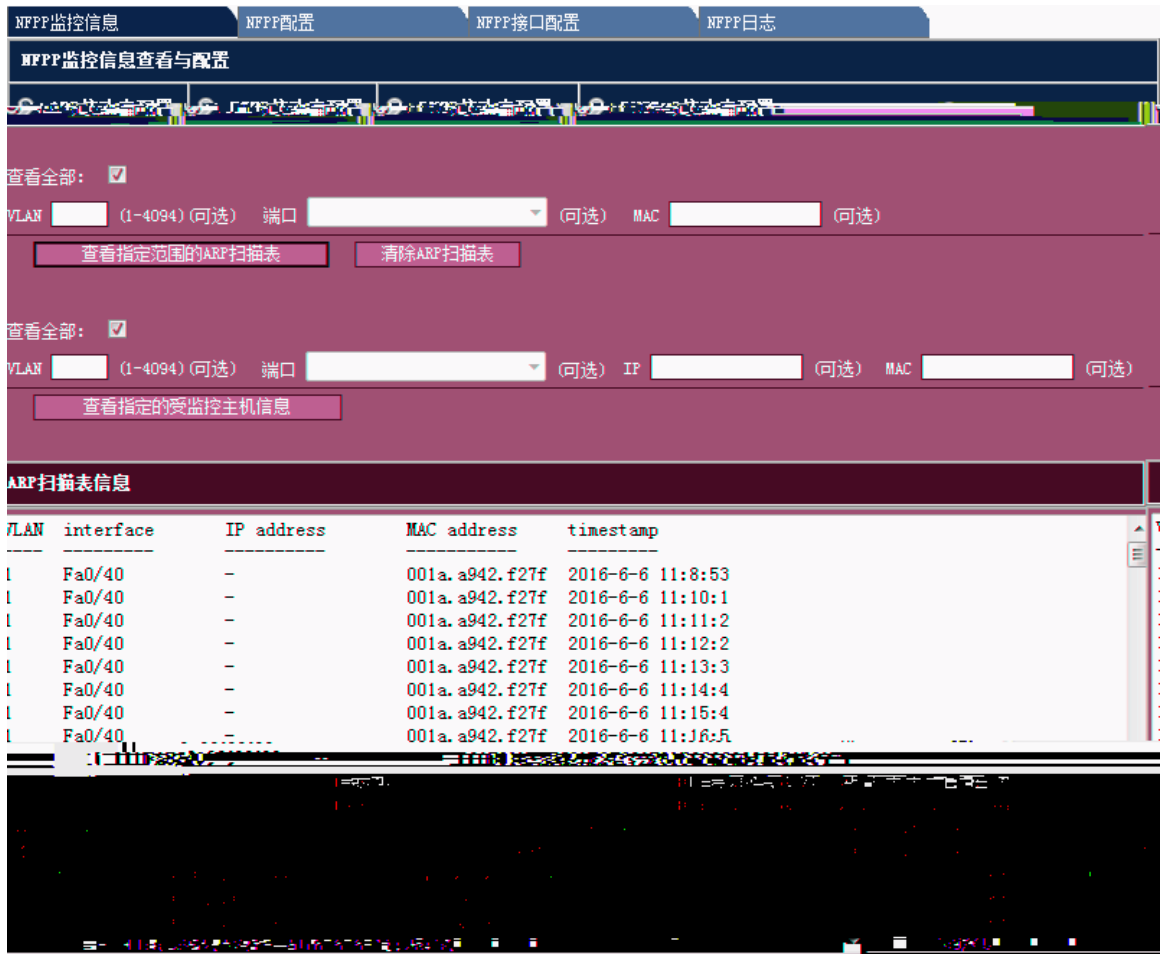
NFPP

1 NFPP



20 NFPP

- ARP



21 ARP

ARP

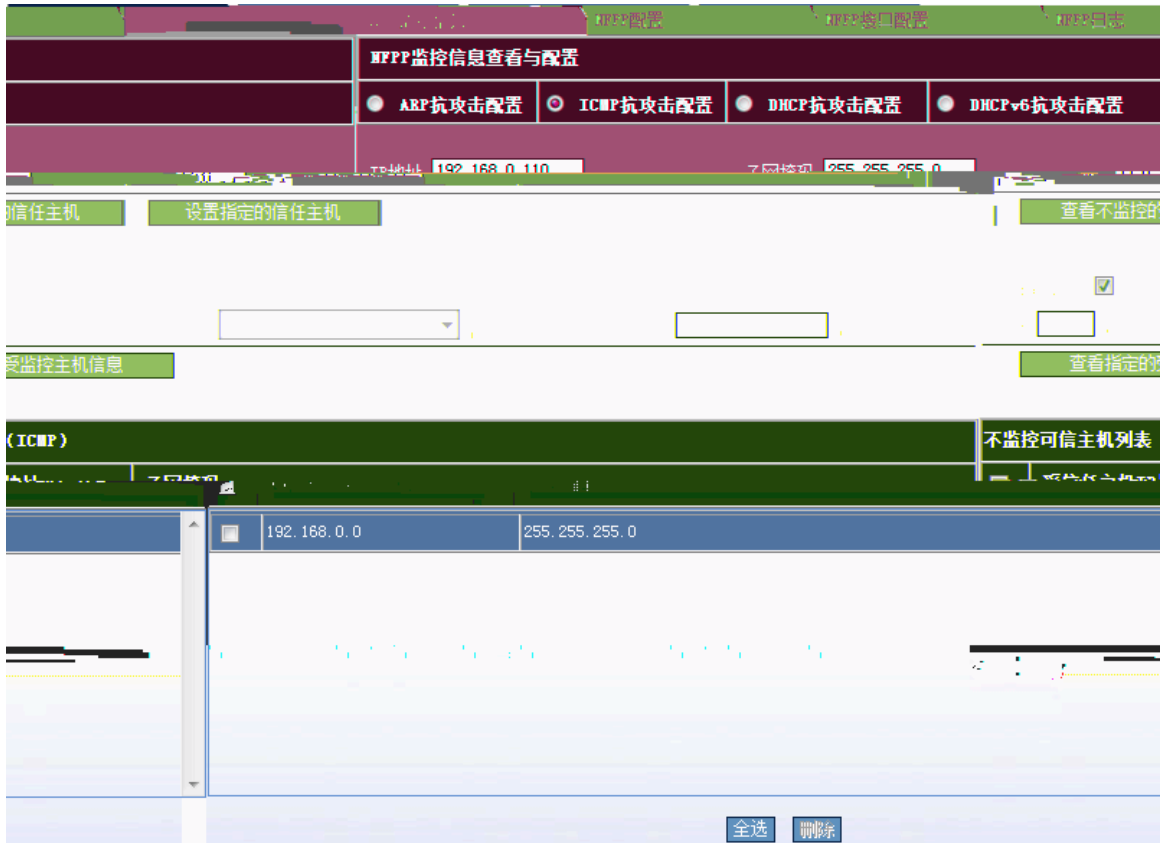
ARP

ARP

ARP

ARP

- ICMP

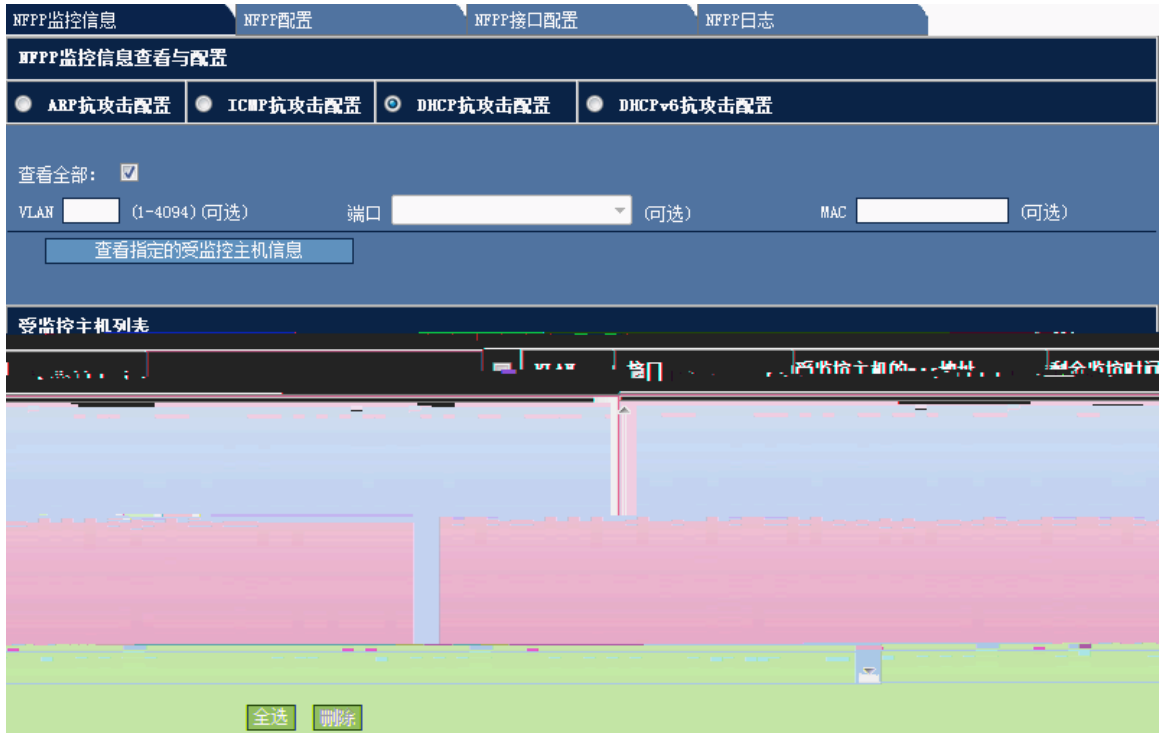


22 NFPF --ICMP

ICMP

IP

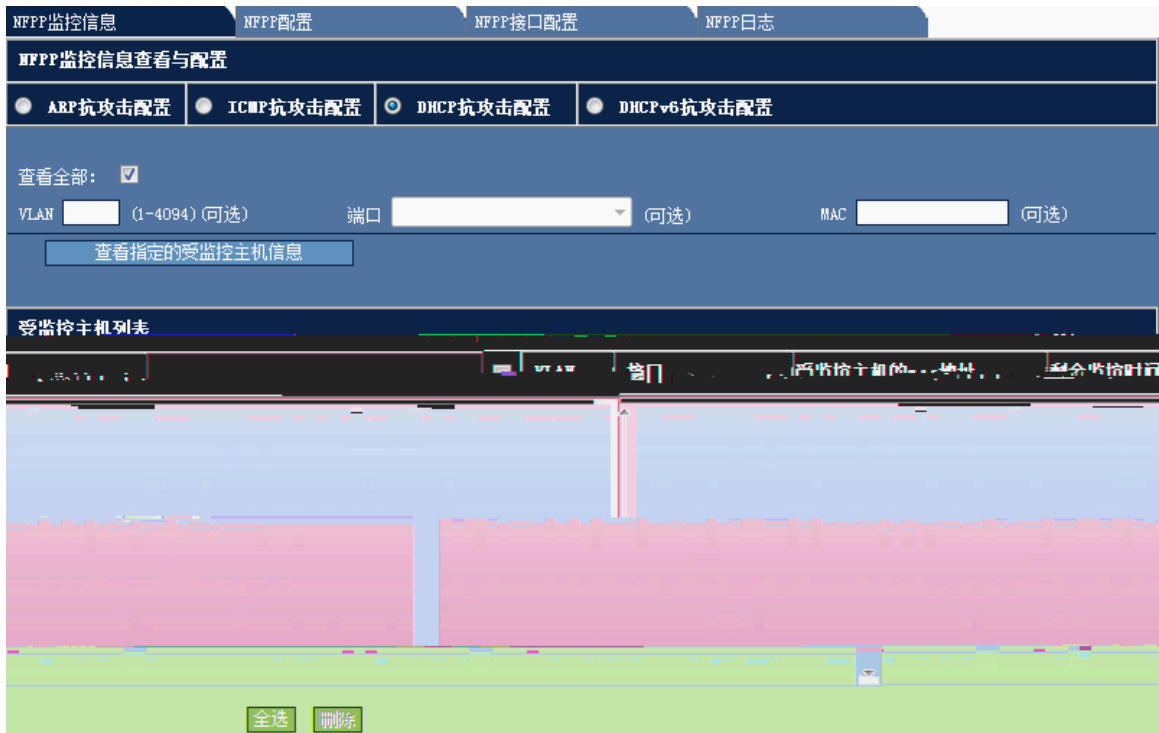
- DHCP



23 NFPP —DHCP

DHCP

● DHCPv6



24 NFPP —DHCP

## DHCPv6

### 2 NFPP

The screenshot displays the 'CPU保护配置' (CPU Protection Configuration) page for NFPP. The page includes a navigation bar with tabs for 'NFPP监控信息', 'NFPP配置', 'NFPP接口配置', and 'NFPP日志'. The main content area contains a table with the following columns: '攻击类型' (Attack Type), '攻击检测' (Attack Detection), '攻击阈值' (Attack Threshold), and '扫描阈值' (Scan Threshold). A tooltip is visible over the '攻击阈值' column, showing '攻击阈值 (基于ip识别/基于mac识别/全局端口):' and '扫描阈值: 15'. The page includes '修改' (Modify) and '恢复默认' (Restore Default) buttons.

攻击类型	攻击检测	攻击阈值	扫描阈值
ARP	Enable	10/300	-
DDoS	Enable	-/10/300	-
DoS	Enable	30/30/30	-
DDoS	Enable	8/8/200	15
DDoS	Enable	100/-/200	-



NFPP监控信息    NFPP配置    **NFPP接口配置**    NFPP日志

**NFPP接口信息配置**

ICMP攻击配置   
 DHCP攻击配置   
 DHCPv6攻击配置   
 DD攻击配置   
 **ARP攻击配置**

0/1     开启ARP攻击     关闭ARP攻击     默认

接口: FastEthernet

(可选): 限速值: 123 (1-9999)    攻击阈值: 123 (1-9999)    基于ip/vid/端口识别主机

(可选): 限速值: 789 (1-9999)    攻击阈值: 789 (1-9999)    基于mac/vid/端口识别主机

(可选): 限速值: 123 (1-9999)    攻击阈值: 456 (1-9999)    基于port端口识别主机(可

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

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	<input type="checkbox"/>	接口	ARP攻击
	123	123/789/123	123/789/456	123	<input type="checkbox"/>	Fa0/1	Enable

全选    删除

28 NFPP    —NFPP    ARP

ARP    NFPP

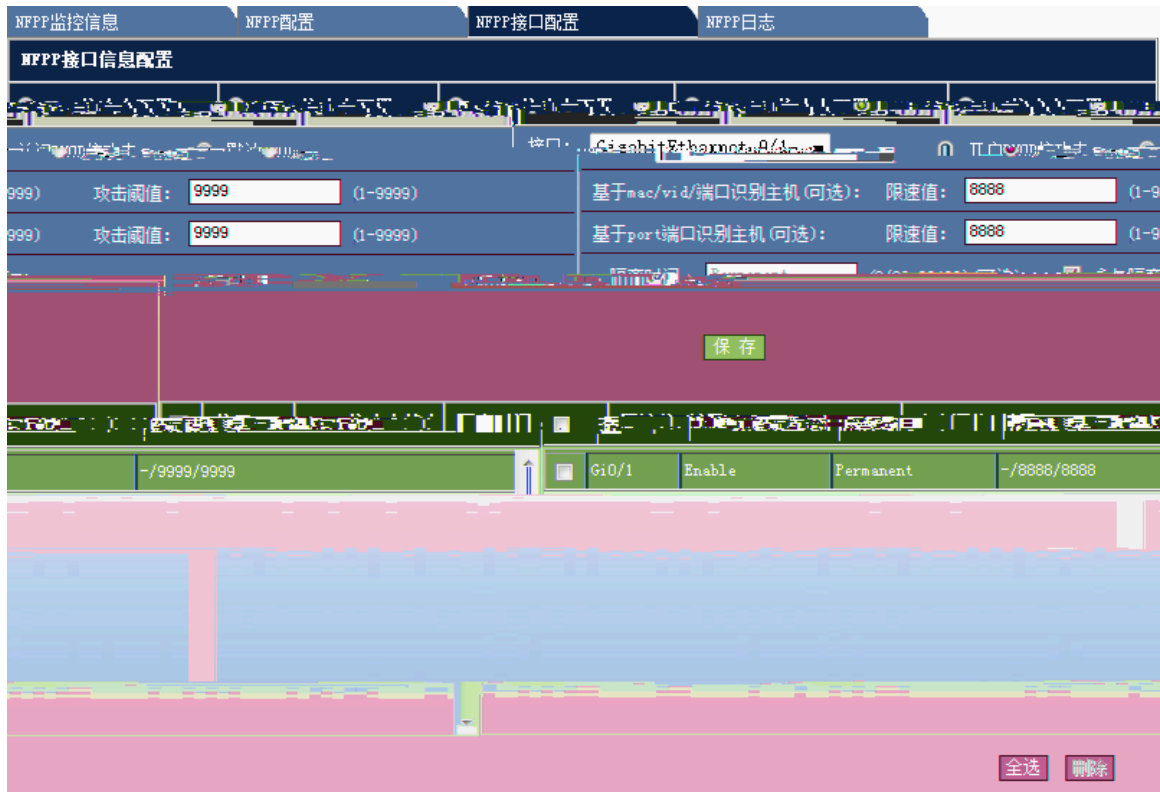
- ICMP



29 NFPF —NFPF ICMP

ICMP NFPF

- DHCP



30 NFPF      —NFPF      DHCP

DHCP      NFPF

- DHCPv6

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**

接口: GigabitEthernet 0/1     开启DHCPv6攻击     关闭DHCPv6攻击

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

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

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

MAC/PORT	接口	DHCPv6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)
	<input type="checkbox"/> Gi0/1	Enable	Permanent	-/8888/8888	-/9999/9999

31 NFPP    —NFPP    DHCPv6

DHCPv6    NFPP

- ND



WEB

**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IP地址(用“|”隔开,指定的区域可用“/”连接):  (0-1000) (可选)

<input type="text" value="1-1000"/>	GigabitEthernet 0/1	<input type="button" value="添加"/>
<input type="text" value="1-1000"/>	GigabitEthernet 0/2	<input type="button" value="删除"/>
<input type="text" value="1-1000"/>	GigabitEthernet 0/3	<input type="button" value="删除"/>

日志缓冲区:	
Timestamp	Protocol VLAN Interface IP address    MAC address    Reason

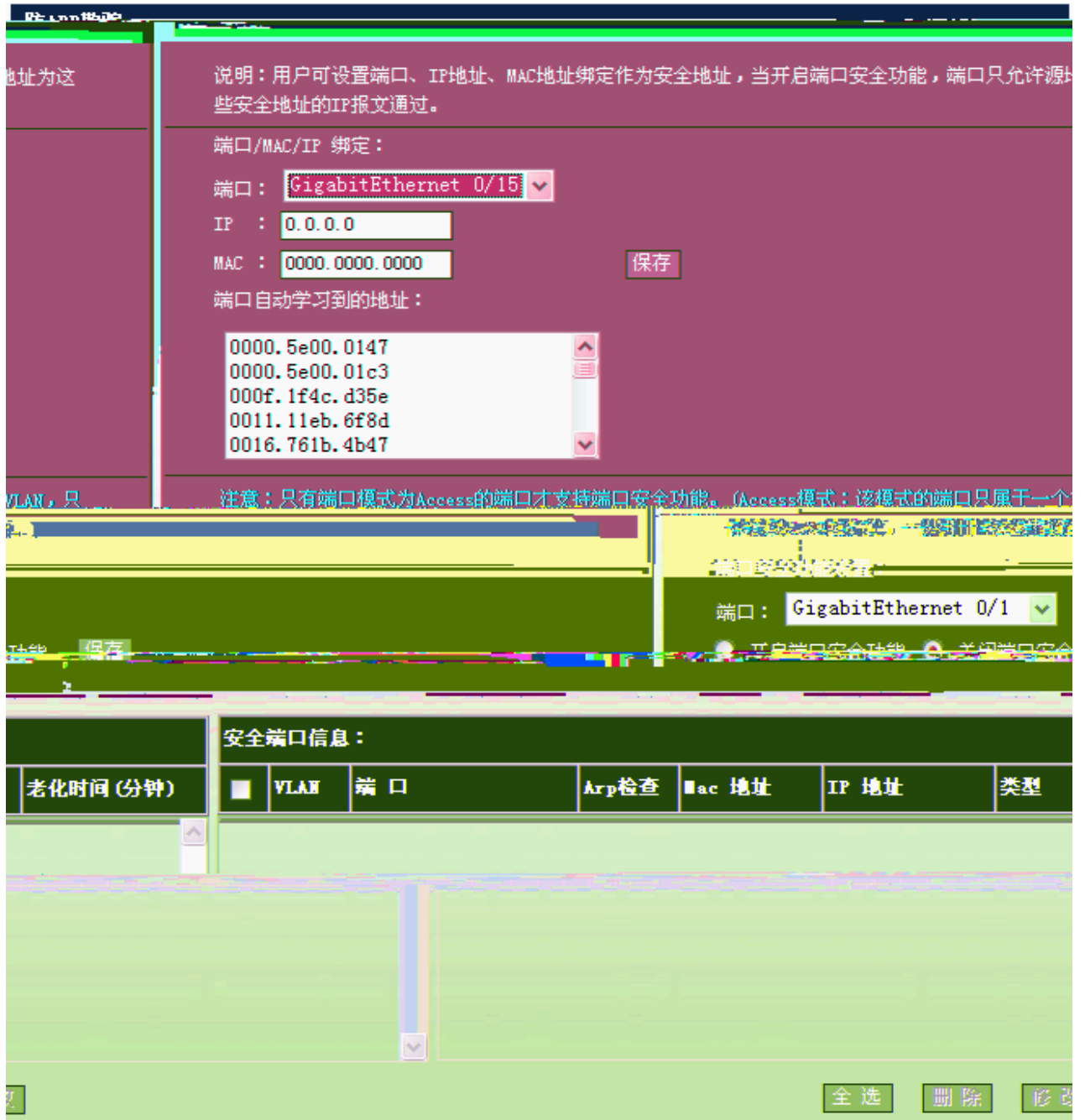
## 2.3

### 2.3.1 ARP

ARP

ARP





36 ARP

1) /MAC/IP

/MAC/IP

IP MAC

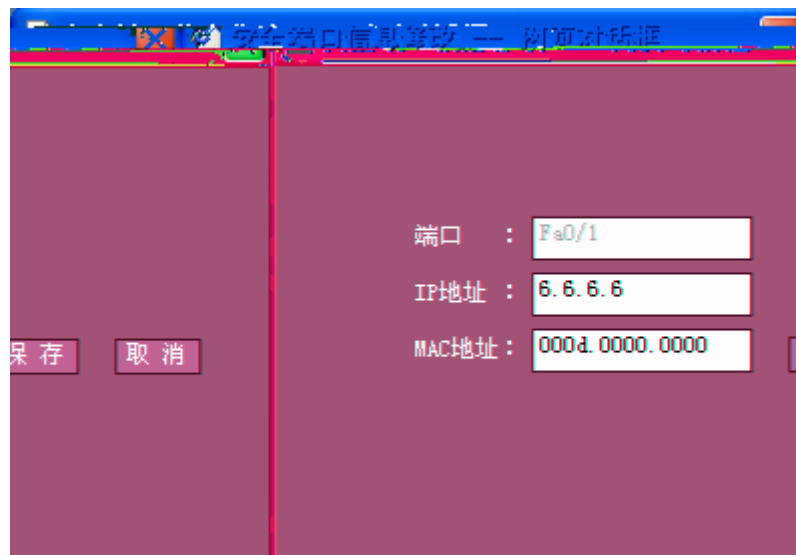
MAC

GigabitEthernet 0/15

MAC

2

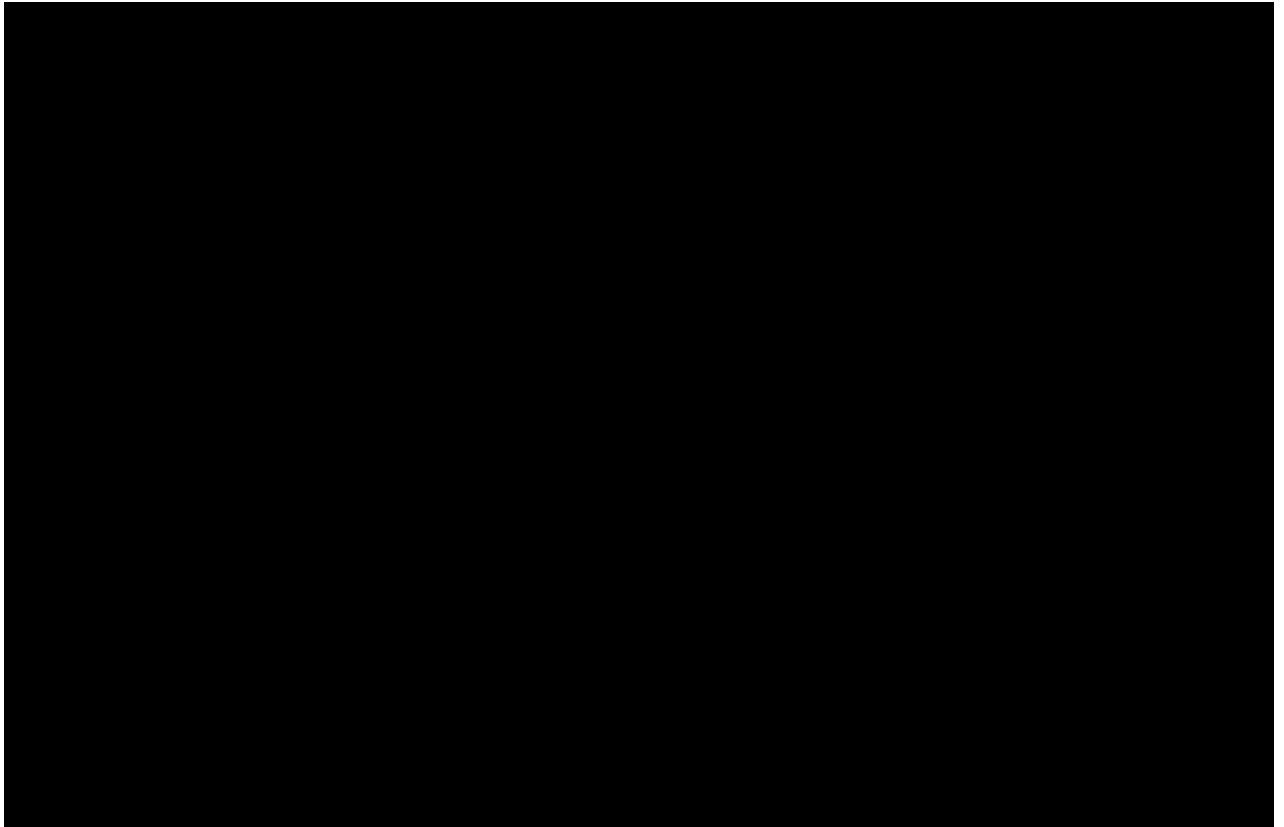
3)



## 2.3.4 ACL

ACL

ACL



39 ACL

1 ACL

ACL

ACL

ACL

ACL

ACE

ACL

ACL

ACE

ACE

2 ACL

IP

IP

IP

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。

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）

扩展访问控制列表：根据数据流的源IP地址制定匹配条件。（编号为100 - 199，2000 - 2699）

禁止

源IP地址: 0.0.0.0

目的IP地址:

保存

ID	源IP地址	目的IP地址	操作
40	IP	IP	禁止



41 IP

ID  
 TCP UDP IP ICMP  
 IP IP IP  
 IP IP IP

3 ACL



42 ACL

ACL

ACL



PC

PC

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

( )

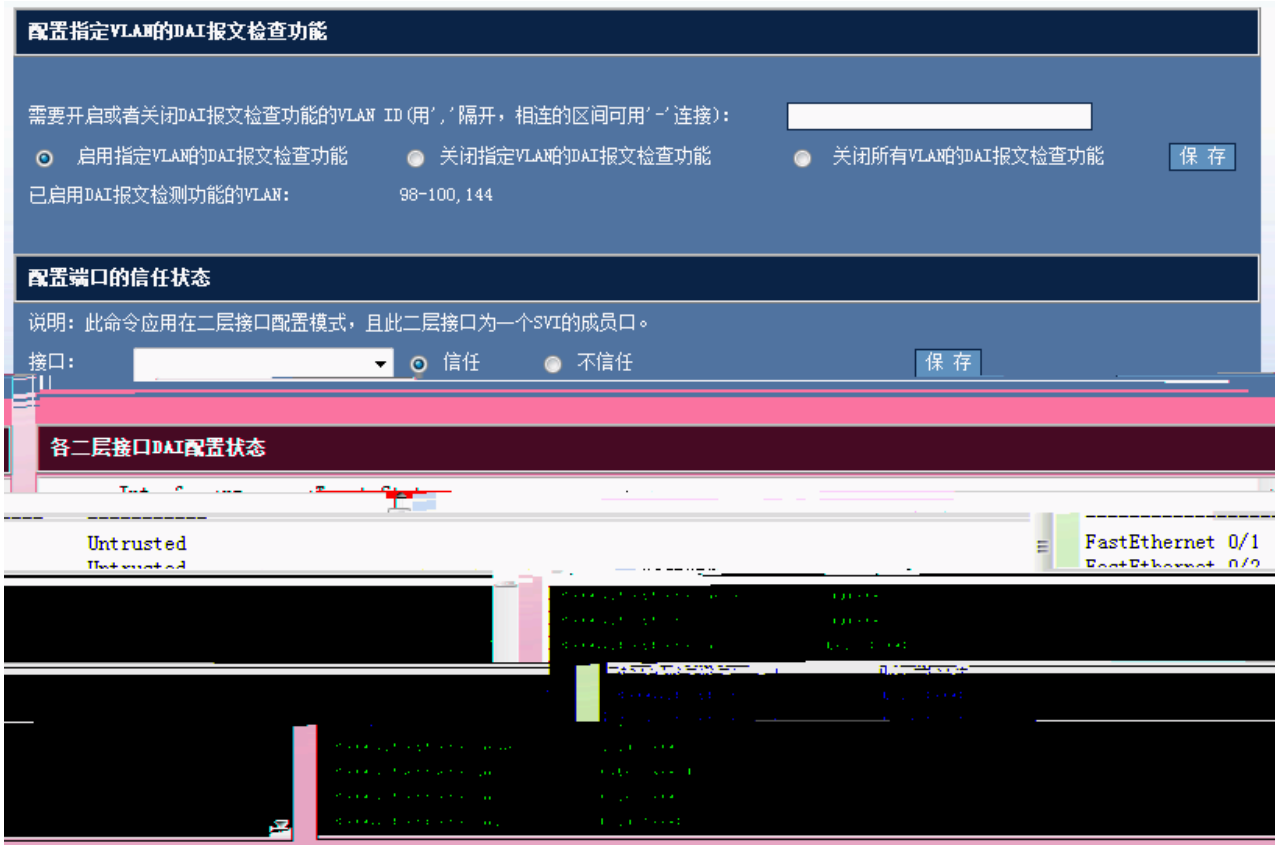
2

IP

MAC

MAC





45 DAI

- 1 VLAN DAI
- VLAN DAI





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	Pos	Pri		
arp-guard	180	7		
arp	180	7		
dot1x	2000	4		
rldp	180	7		
180	7			
180	7			
180	7			
tunnel-bpdu	180	6		
ipv4-icmp-local	1600	6		
lldp	180	5		
lldp_cdp	180	5		
cfm-pdu	180	3		

49

管理板/单机/堆叠系统的接收报文的统计信息				
Type	Pps	Total	Drop	
arp	10	324430	0	
arp-guard	180	180	0	
dot1x	2000	2000	0	
rldp	180	180	0	
180	7	180	0	
180	7	180	0	
180	7	180	0	
tunnel-bpdu	180	180	0	
ipv4-icmp-local	1600	1600	0	
lldp	180	180	0	
lldp_cdp	180	180	0	
cfm-pdu	180	180	0	

### 2.3.9 RADIUS

#### RADIUS

##### 1 RADIUS

Radius服务器组

**AAA参数配置**

AAA new-model:  开启  关闭

密钥: 隐藏密钥  保存

记帐计费更新功能:  开启  关闭

IP授权模式: supplicant 保存

**Radius服务器**

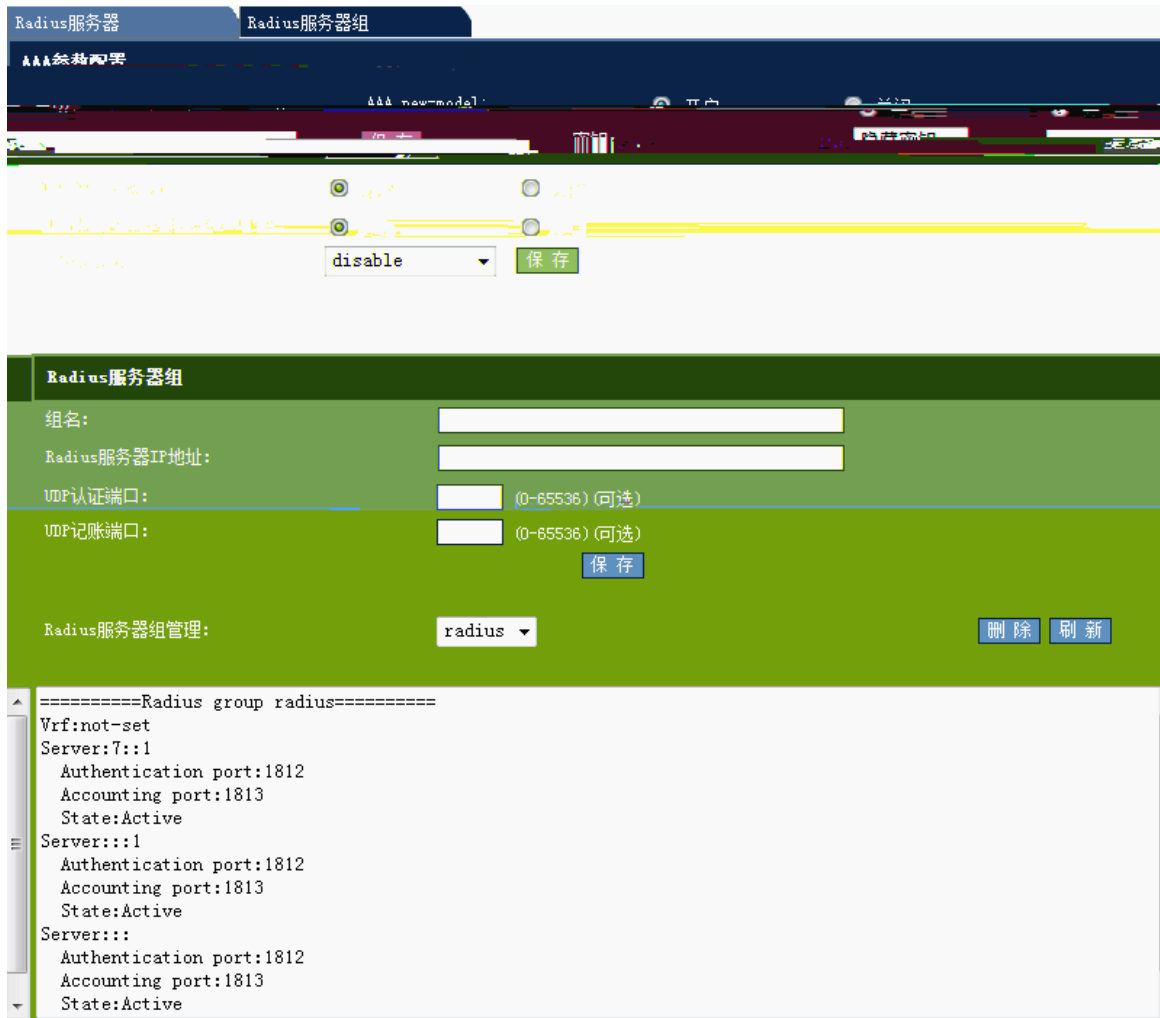
Radius服务器IP地址: 192.168.0.111

UDP认证端口:  (0-65535) (可选)

UDP记帐端口:  (0-65535) (可选) 保存

Radius服务器IP地址	认证端口	记帐端口	服务器状态
192.168.0.111	1813	1812	

全选 删除



### 52 RADIUS

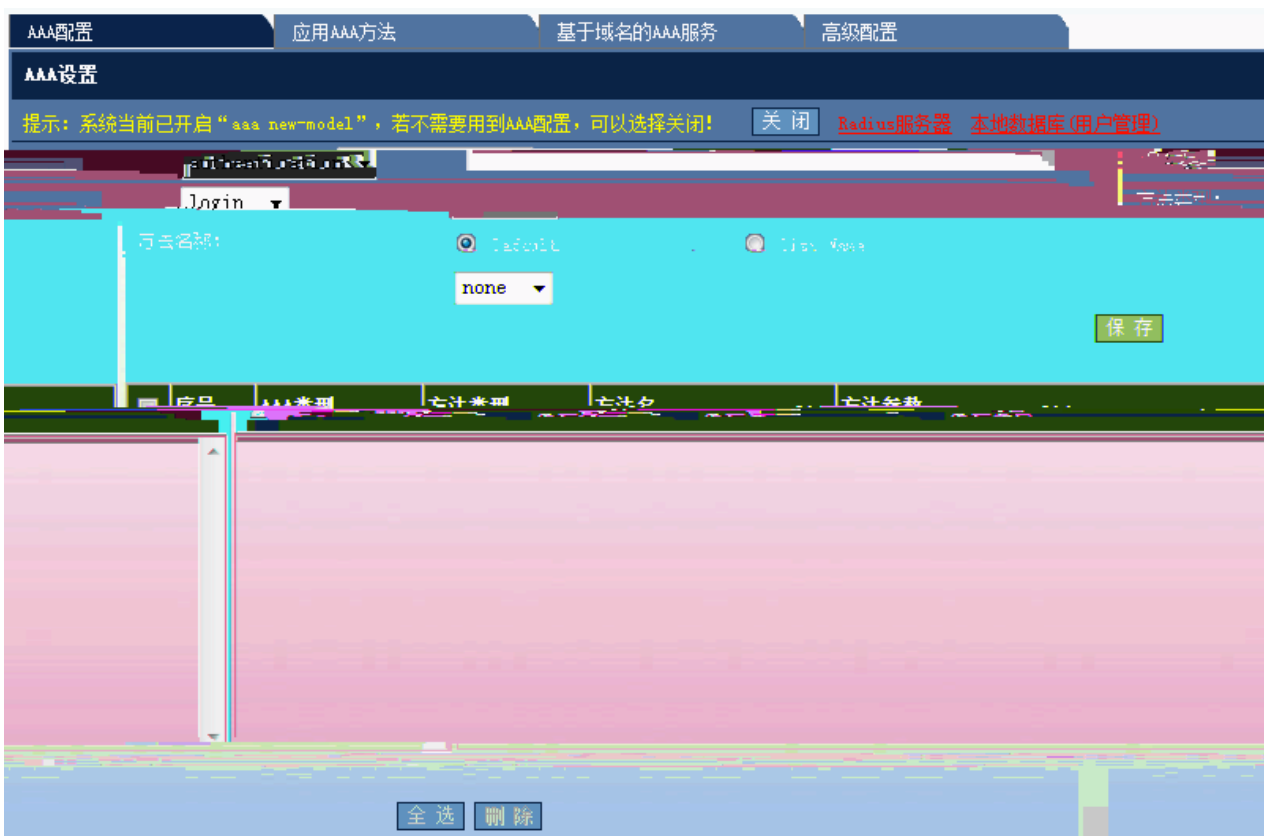
RADIUS IP

Radius

### 2.3.10 AAA

AAA

AAA



53 AAA

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



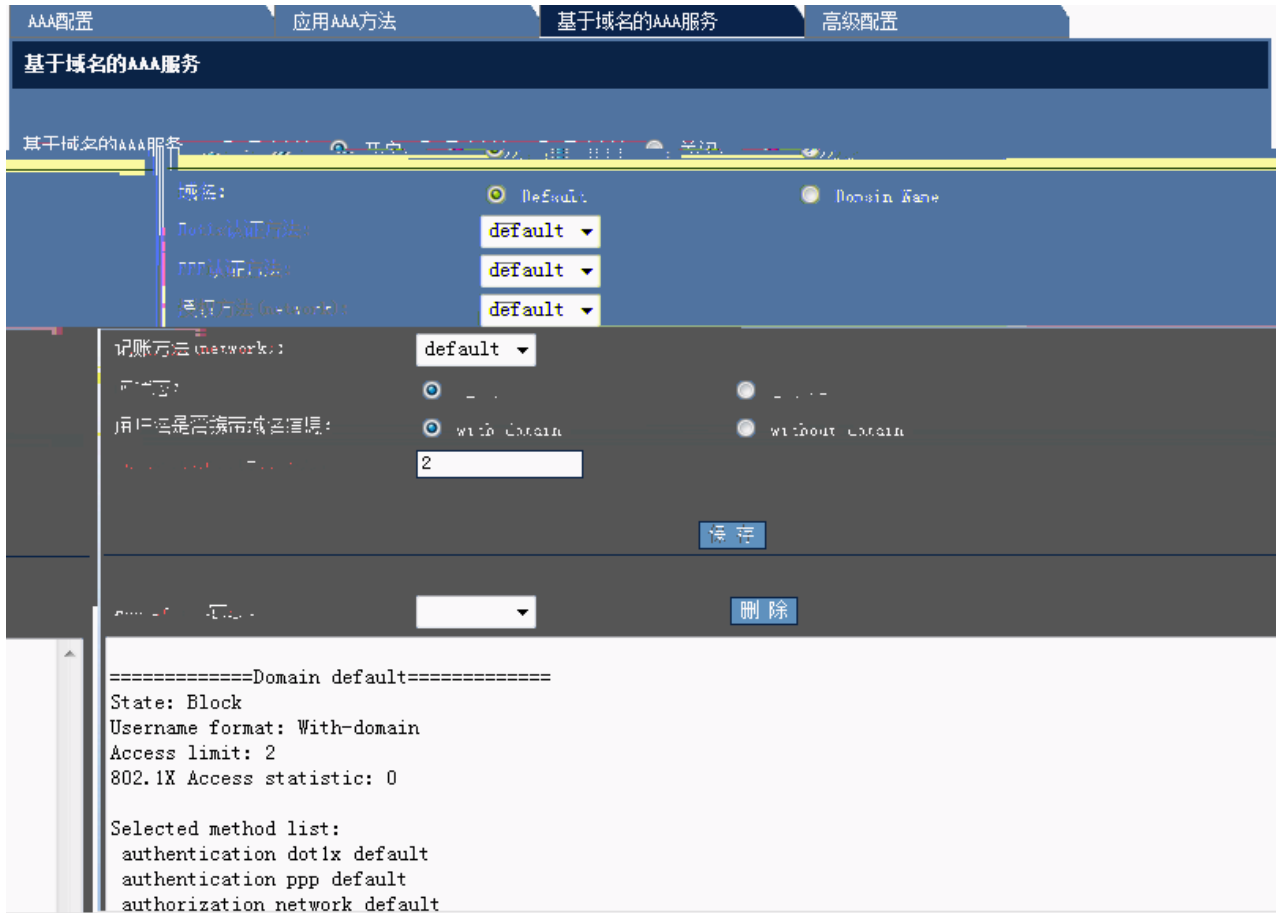
54 AAA

AAA

AAA

3

AAA



55

AAA

(network)

AAA  
(network)

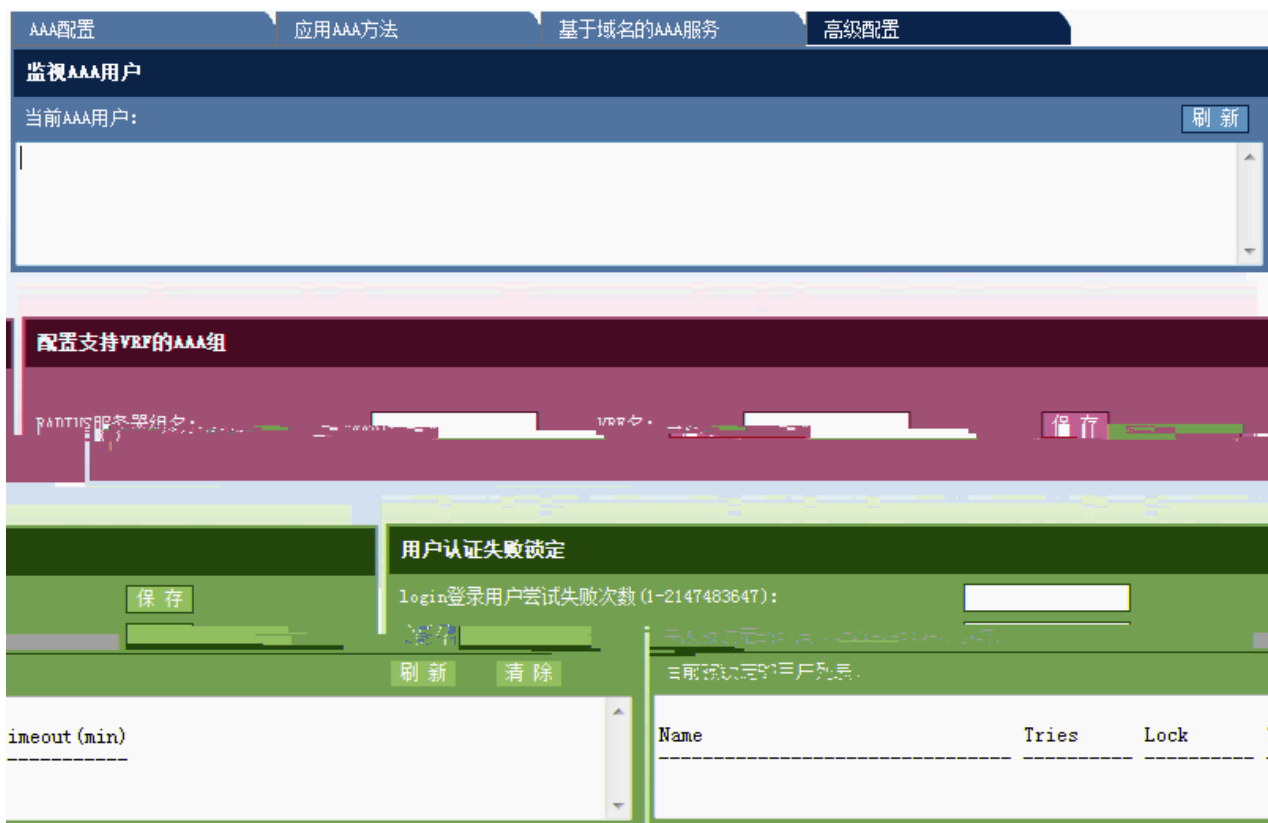
Dot1x

PPP

Access Limit

AAA Domain

4 AAA



56 AAA

AAA

AAA

VRF AAA

### 2.3.11 Dot1x

#### Dot1x

##### 1 Dot1x



57 Dot1x

Dot1x





60

2

802.1x

MAC

VLAN

### 2.3.12



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.f866.66e0	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

WEB



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:    IP Only Mode   

<input type="checkbox"/>	序号	端口	IP Only Mode
<input type="checkbox"/>	1	FastEthernet 0/1	YES
<input type="checkbox"/>	2	FastEthernet 0/3	YES

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

Empty content area with a vertical scrollbar.

67

IP

## 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

---

**DHCP Snooping 信任端口设置**

端口：

---

**DHCP Snooping配置信息**

	端口	信任端口
限速		

68 DHCP Snooping

#### 1)DHCP Snooping

2)DHCP Snooping

## 2.4 QOS

### 2.4.1



69

ACL

### 2.4.2



## 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
<input type="checkbox"/>	FastEthernet 0/1	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/2	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/3	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/4	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/5	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/6	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/7	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/8	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/9	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/10	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/11	-	-	-	-

## 2.4.4



73

1)

Static

Sticky Mac

2)

Mac

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:

接口	MAC地址	Vlan ID	IP地址
FastEthernet 0/1	1000.0000.0000	10	1.2.3.3

75

Mac      VLAN ID      IP      MAC      Vlan

## 2.5

### 2.5.1

系统信息	
设备型号 :	S2924G
主机名 :	Ruijie
软件版本 :	RGOS (Ruijie) Business Edition Release 10.2.00(3) [Copyright © 2008 Ruijie Systems, Inc.]
硬件版本 :	LC7T
MAC地址 :	001E1010B041

76

## 2.5.2

```
当前配置
Building configuration...
Current configuration : 12931 bytes
!
version RGNOS 10.2.00(3), Release(30355
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	800	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

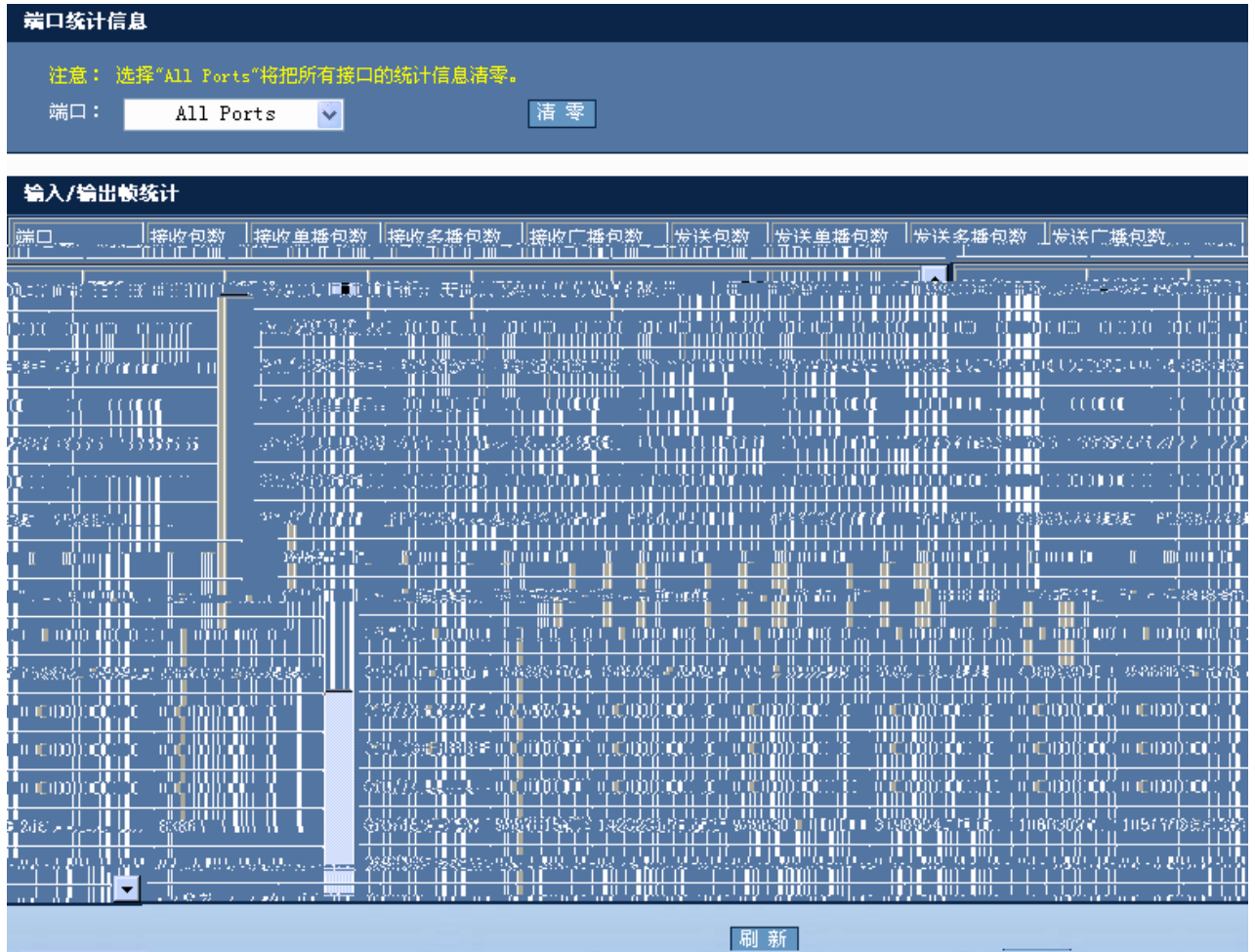
## 2.5.4

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

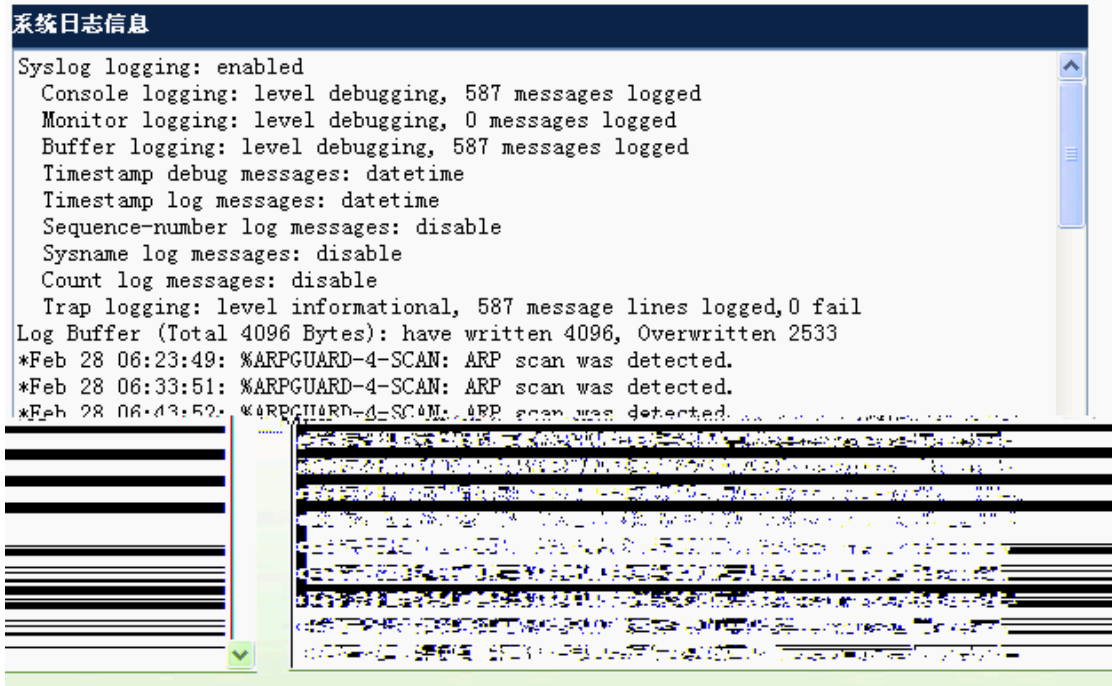
79

## 2.5.5



80

## 2.5.6



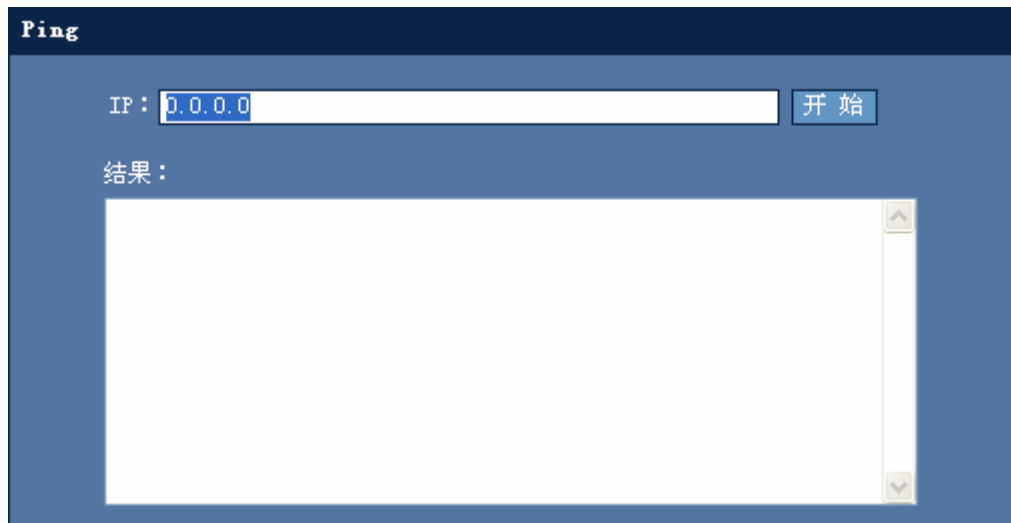
81

## 2.6

### 2.6.1 Ping

Ping

Ping



82 Ping

IP

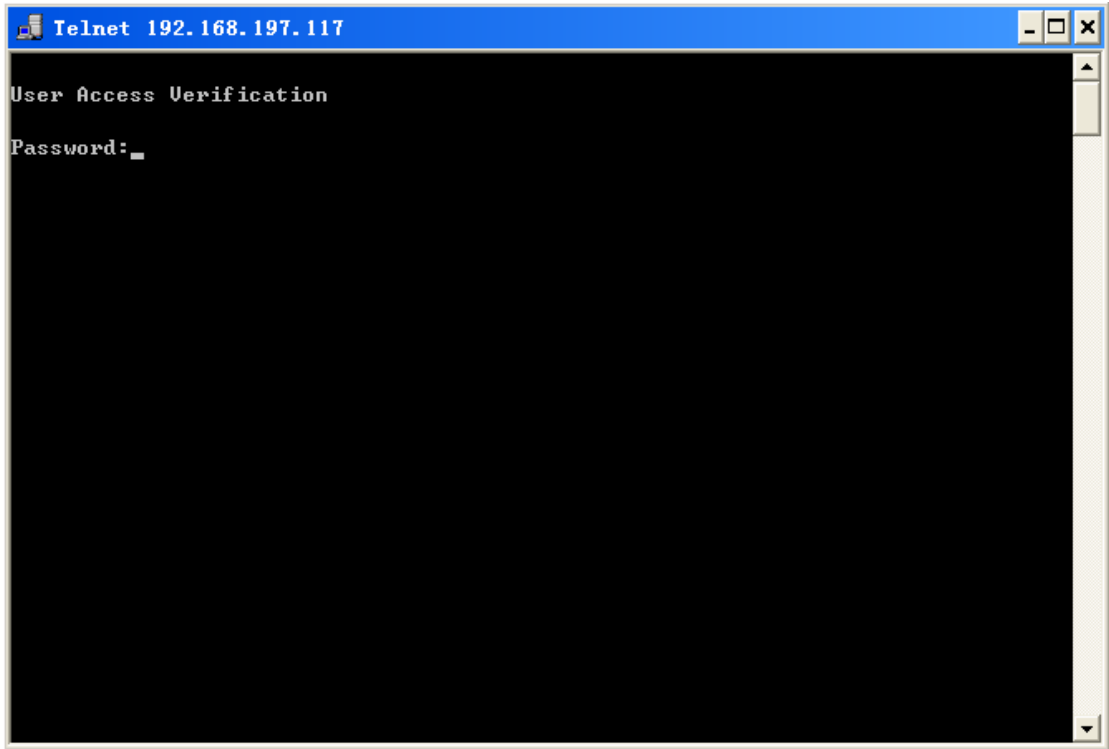
IP

Ping

## 2.6.2 Telnet

Telnet

Telnet



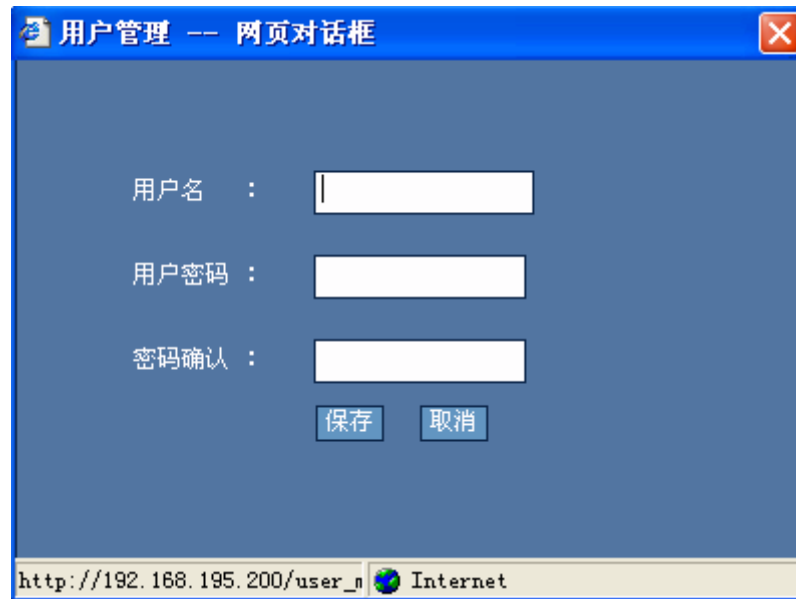
83 Telnet

PC Telnet Telnet Telnet PC Telnet

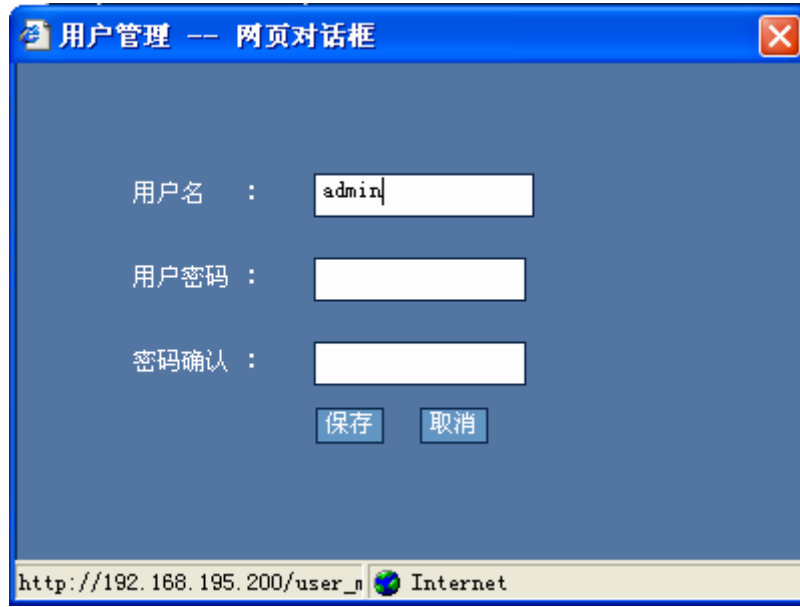
## 2.6.3



84



85



86



#### 2.6.4

**修改Enable口令**

注意：如果您设置了新的Enable口令，则在设置之后使用新口令重新登录。

新口令：

确认新口令：

保存

---

**修改Telnet登录口令**

新口令：

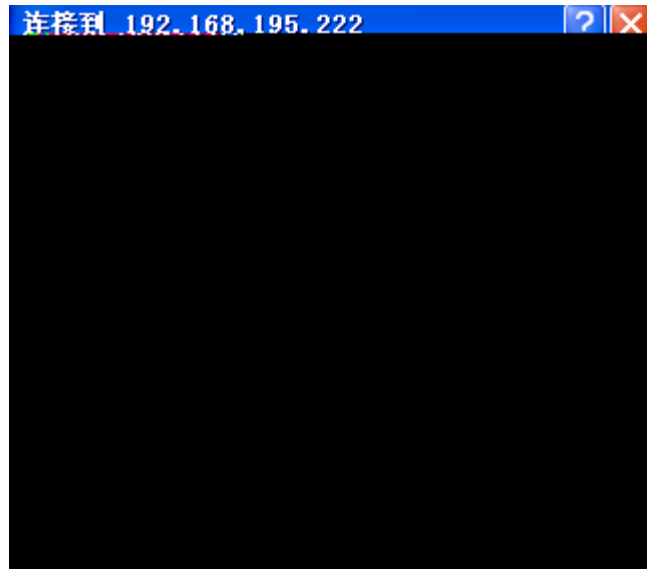
确认新口令：

保存

87

1) Enable

Enable



88

2) Telnet

Telnet

2.6.5 /



89 /

config.text

TFTP

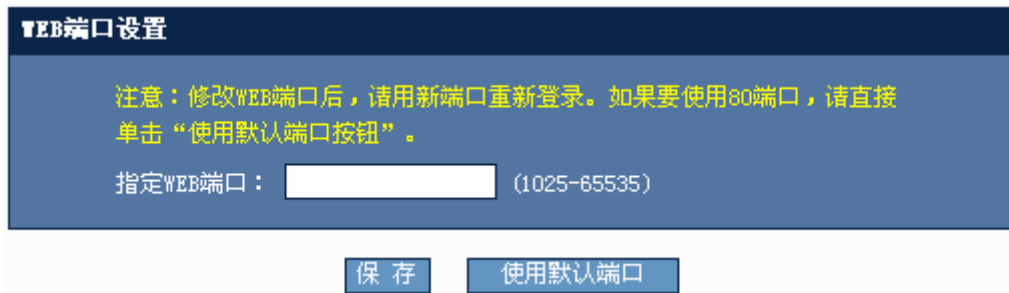
IP

TFTP

2.6.6 WEB

WEB

WEB



90 WEB

8080 IP 192.168.1.1 <http://192.168.1.1:8080>



**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
```