

WEB a Â Õ Å

RG-AS2GT x æ @ & ²

RGOS 10.4(2b12)p4

g é • - Y u V1.0

ø W

• y f

RGOS 10.4 (2b12)p4

~ À * Š

ê ± V

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

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

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

7 24

4008-111-000

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

service@ruijie.com.cn

ü » ž j

- / ,

1)

[] []

{x|y|...}

[x|y|...]

//

2)

1 WEB

WEB

IE

WEB

WEB

WEB

WEB

WEB

WEB

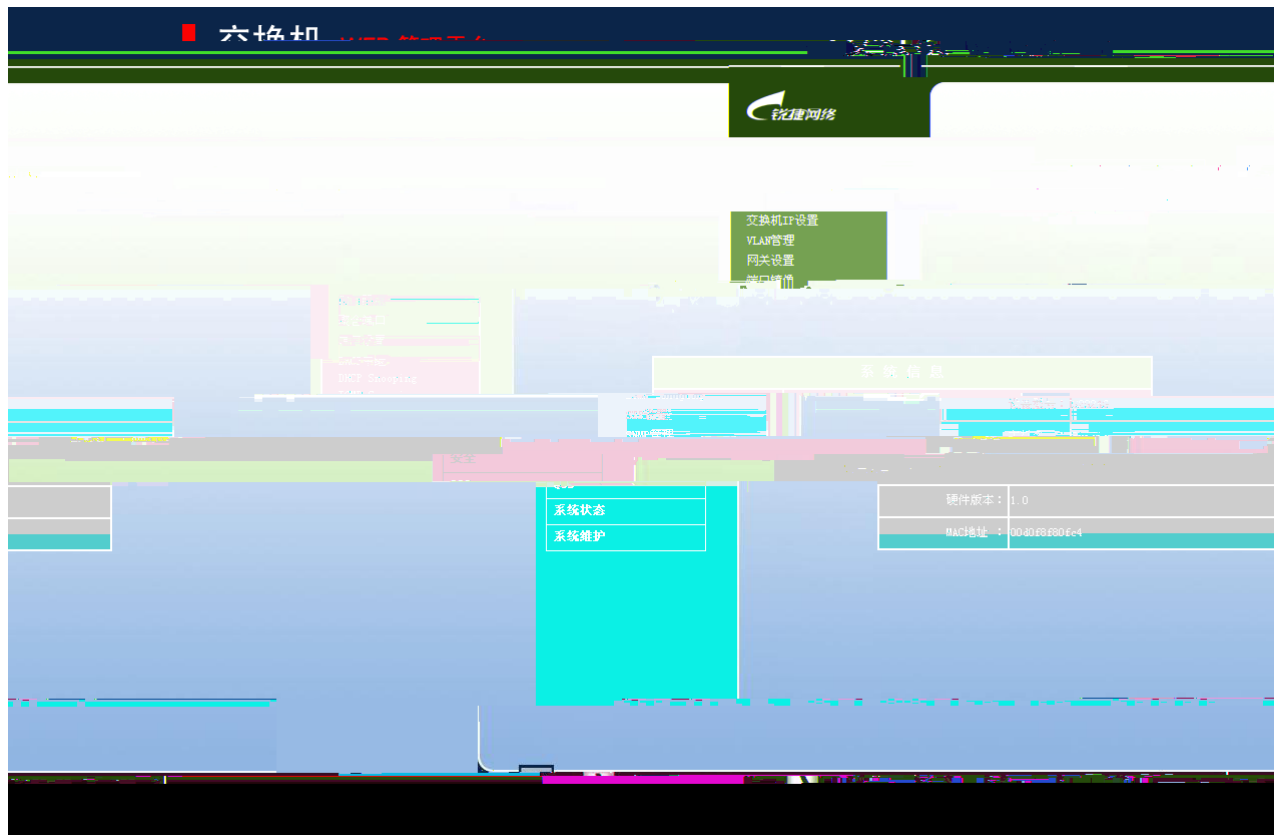
IE

2



2

WEB

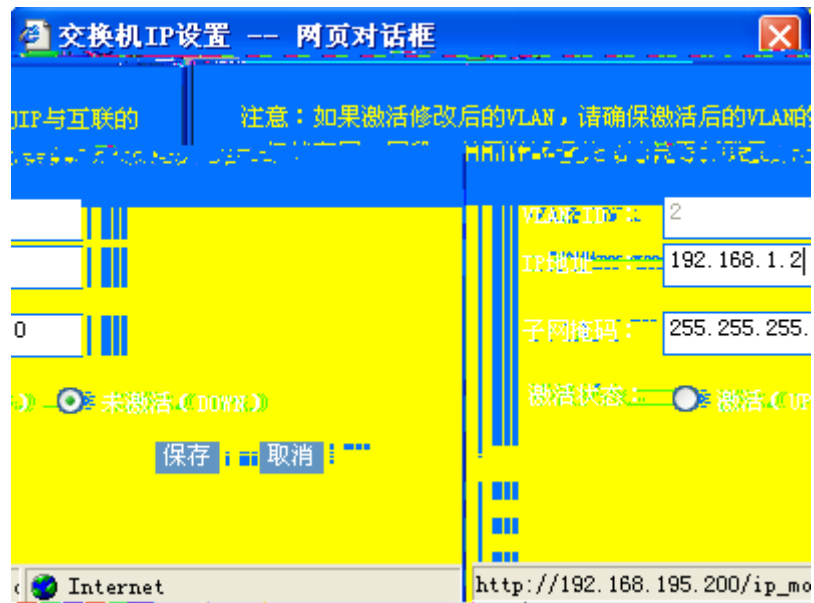


3 WEB



WEB





5 IP

IP

2.2.2 VLAN

VLAN

1 VLAN

VLAN管理 指定VLAN

说明：VLAN是虚拟局域网（Virtual Local Area Network）的简称。它是在一个物理网络上，实现逻辑上不同的用户。属于不同VLAN的用户无法进行二层通讯。

名称	<input type="checkbox"/>	VLAN ID	VLAN 名称	状态
IC	<input type="checkbox"/>	1	VLAN0001	STAT
IC	<input type="checkbox"/>	2	VLAN0002	STAT

新建 全选 删除 修改

6 VLAN

VLAN

VLAN

VLAN

VLAN管理 -- 网页对话框

VLAN ID : (1-4094)

VLAN 名称 : (可选)

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

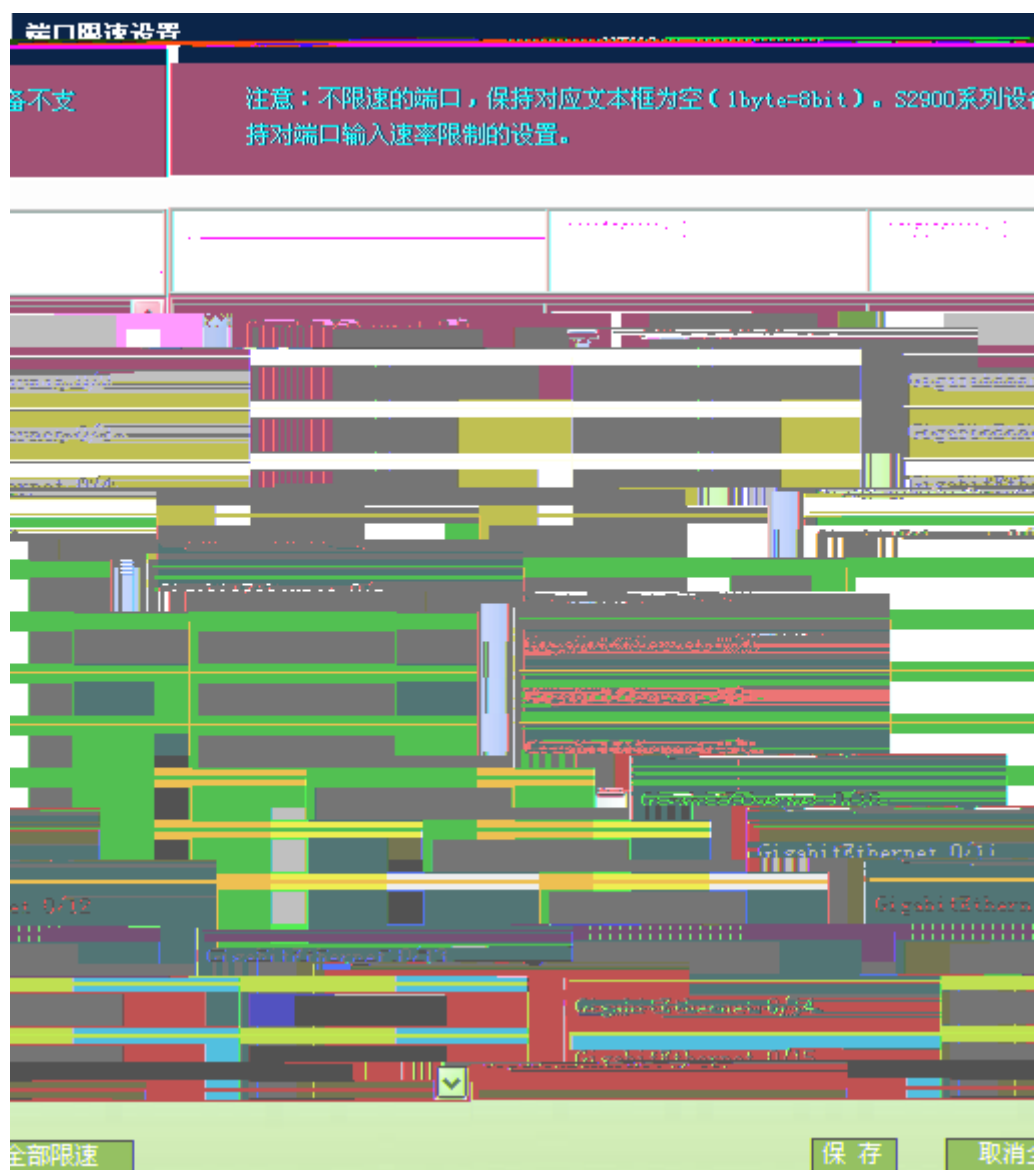
9 VLAN

VLAN ID

2.2.3

11

2.2.5



12

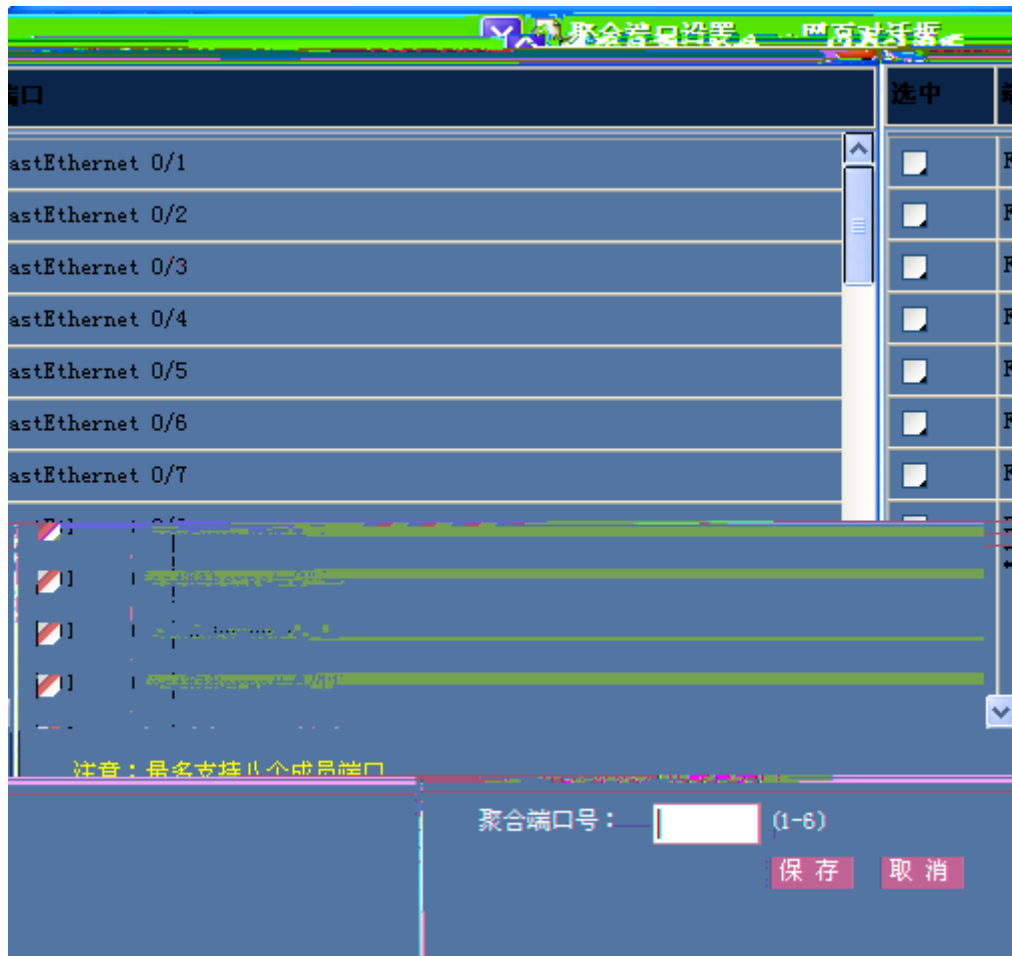
2.2.6



13

1

2



14

3

2.2.7

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	Full	100	Off	-
Gi0/3	Down	Full	100	Off	-
Gi0/4	Down	Full	100	Off	-
Gi0/5	Down	Full	100	Off	-
Gi0/6	Down	Full	100	Off	-
Gi0/7	Down	Full	100	Off	-
Gi0/8	Down	Full	100	Off	-
Gi0/9	Down	Full	100	Off	-
Gi0/10	Down	Full	100	Off	-
Gi0/11	Down	Full	100	Off	-
Gi0/12	Down	Full	100	Off	-

15

2.2.8 DHCP

DHCP

DHCP



16 DHCP

1) / DHCP

/ DHCP

2) DHCP

DHCP

DHCP

2.2.9 IGMP Snooping

IGMP Snooping

IGMP Snooping



SNMP



19 SNMP

SNMP

SNMP

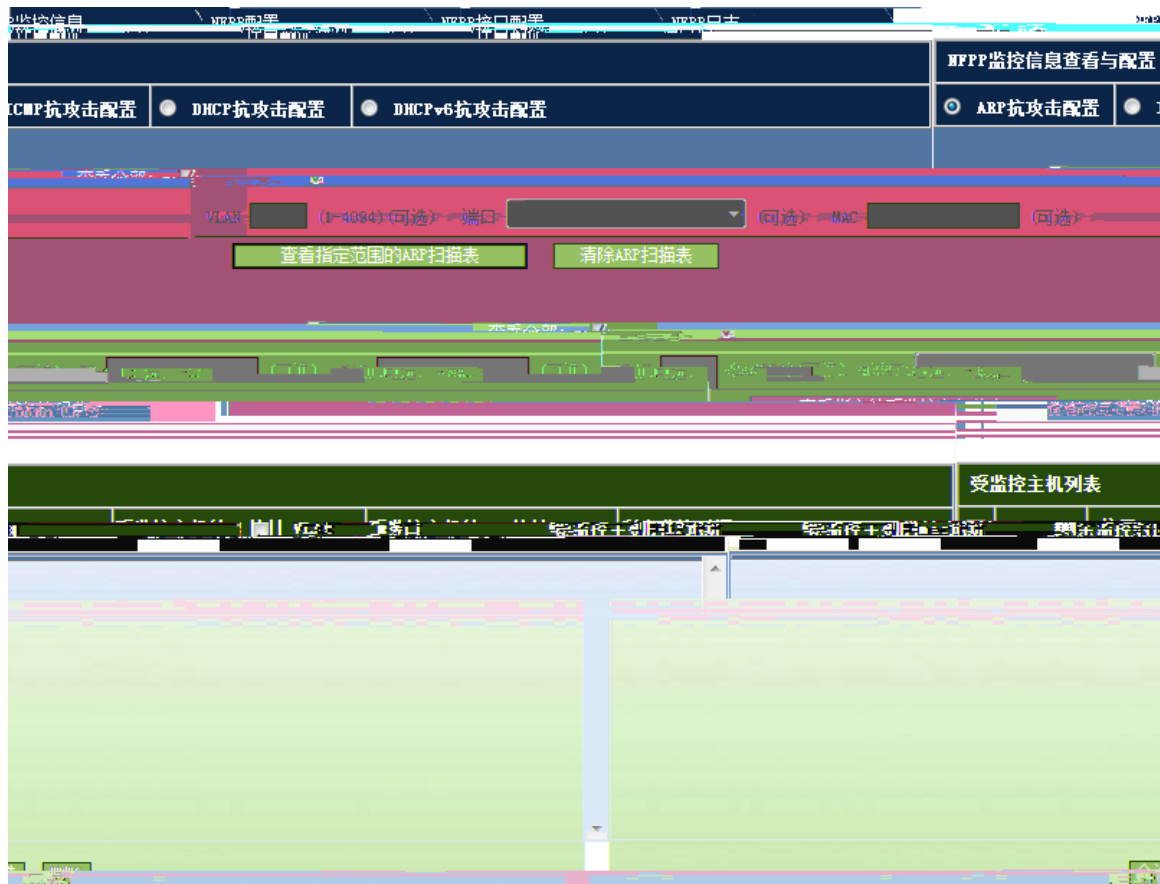
SNMP

SNMP

2.2.12 NFPP

NFPP

1 NFPP



20 NFPP

- ARP

清除ARP扫描表 查看指定范围的ARP扫描表

查看全部:

(可选) MAC (可选) VLAN (1-4094) (可选) 端口

查看全部:

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

查看指定的受监控主机信息

ARP扫描表信息				
VLAN	interface	IP address	MAC address	timestamp
1	Fa0/40	-	001a.a942.f27f	2016-6-6 11:8:53
1	Fa0/40	-	001a.a942.f27f	2016-6-6 11:10:1
	001a.a942.f27f	2016-6-6 11:11:2		Fa0/40
	001a.a942.f27f	2016-6-6 11:12:0		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 11:21:21		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

21 ARP

ARP

ARP

ARP

ARP

ARP

ARP

- ICMP



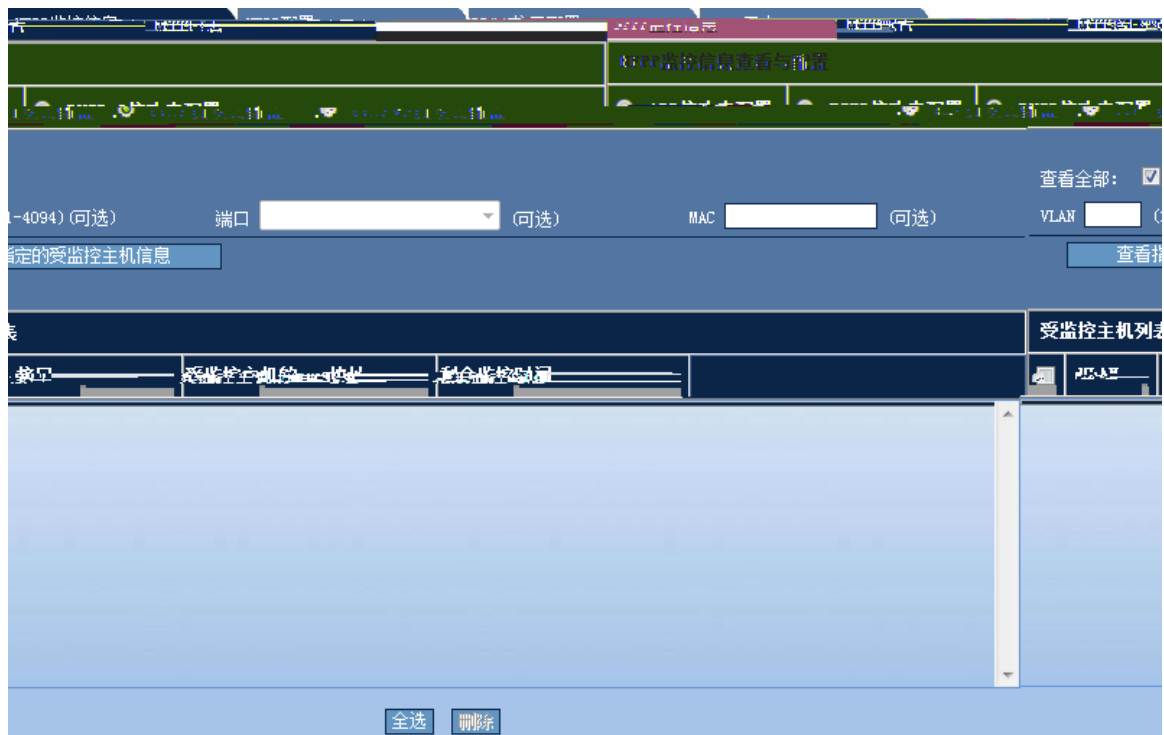
22 NFPP

--ICMP

ICMP

IP

- DHCP



23 NFPP — DHCP

DHCP

- DHCPv6

NFPP监控信息 NFPP配置 NFPP接口配置 NFPP日志

比例	Protocol报文最大带宽	Route报文最大带宽	Manage报文最大带宽	Protocol报文比例	Route报文比例	Manage报文比例
-	-	-	-	-	-	-

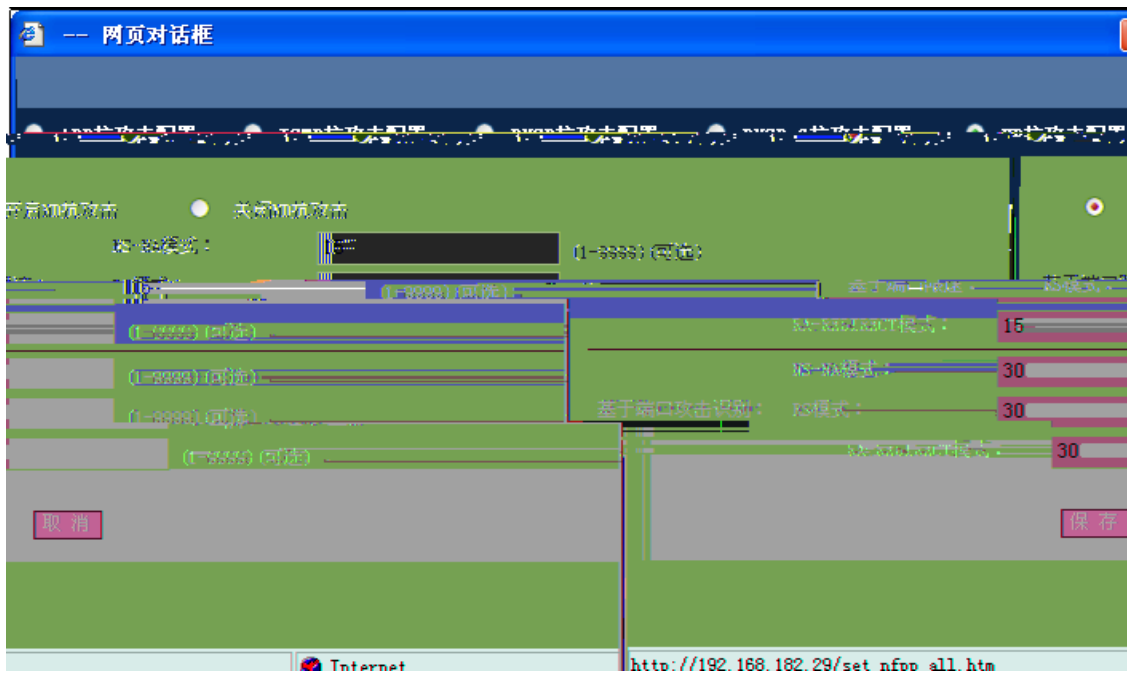
修改 恢复默认

协议类型: ARP ICMP DHCP DHCPv6

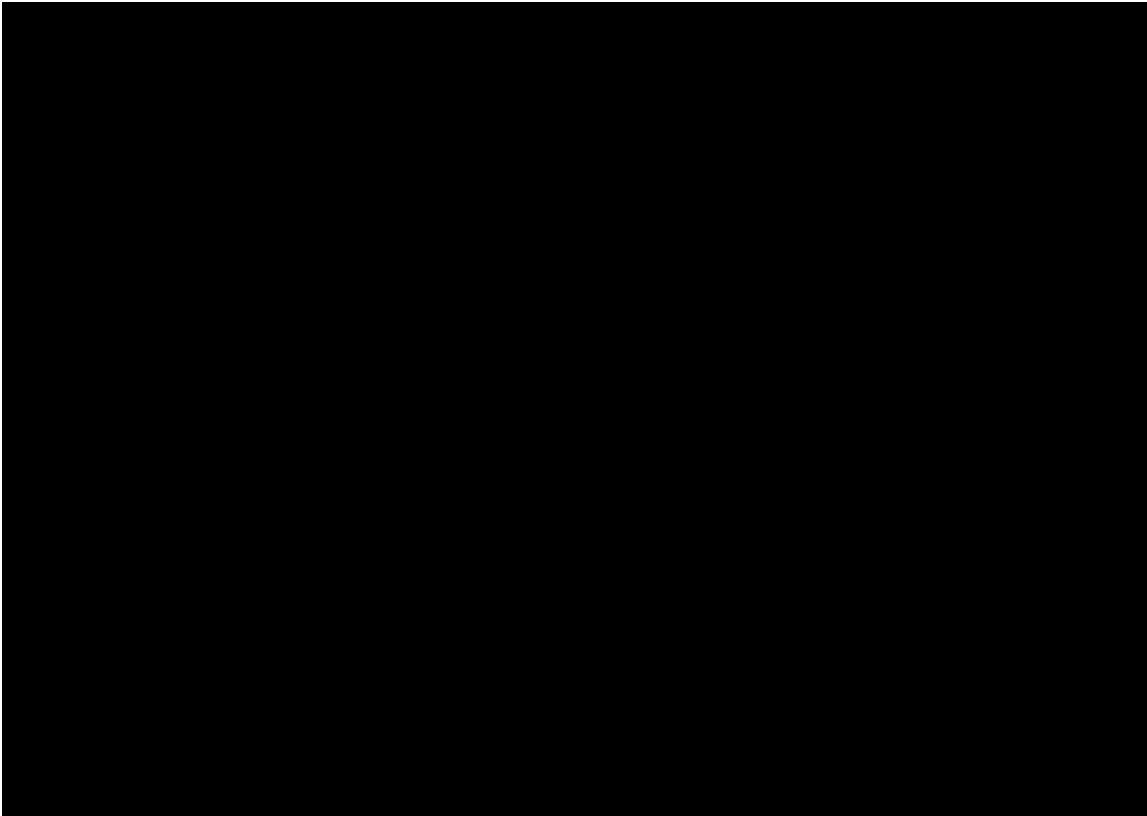
协议类型	状态	隔离时间	监控时间	最大监控主机数	基于IP识别限速/基于mac识别限速/全局端口限速	攻击阈值 (基于ip识别/基于mac识别/全局端口)	扫描阈值	恢复默认值
Enable	Enable	0	600s	1000	4/4/100	8/8/200	15	恢复默认
0	0	600s	600s	1000	100/-/200	100/-/200	-	恢复默认
-/5/150	-/5/150	15/15/15	-	-	-	-	-	恢复默认
-/10/300	-/10/300	30/30/30	-	-	-	-	-	恢复默认
-	-	-	-	-	-	-	-	恢复默认

恢复默认 修改

25 NFPP NFPP 4



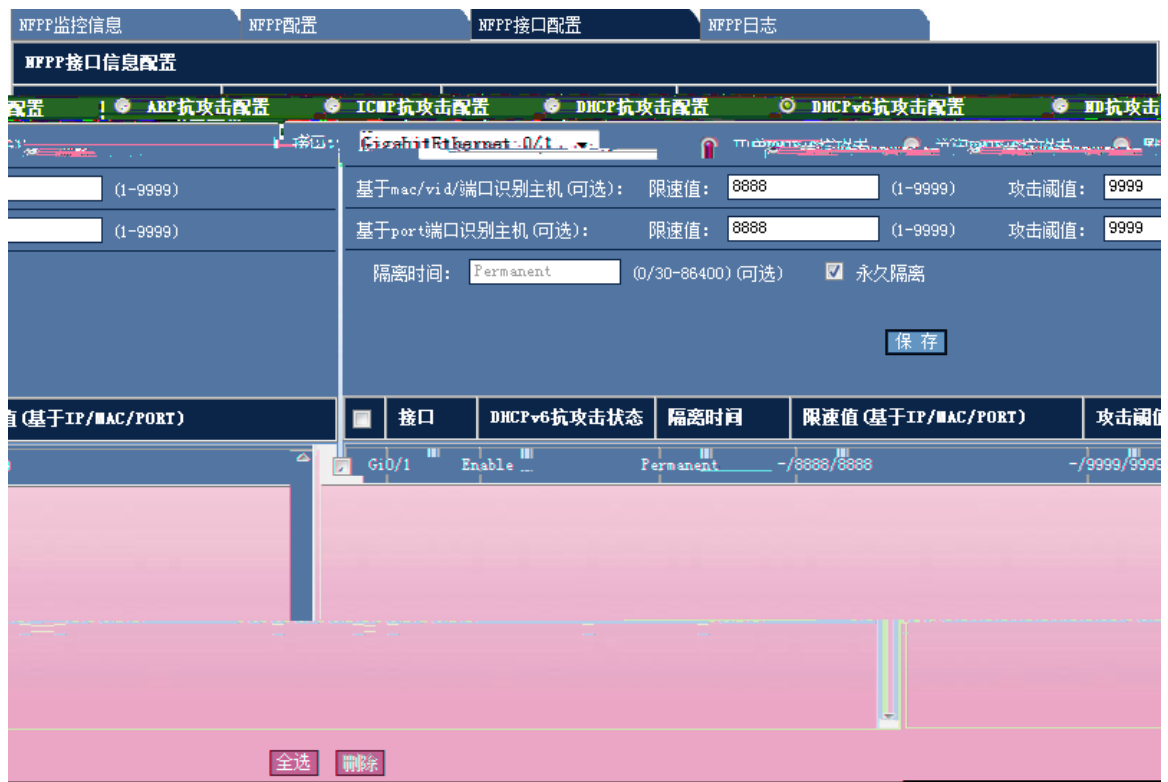
27 NFPF



28 NFPP —NFPP ARP

ARP NFPP

- ICMP



31 NFPF — NFPF DHCPv6

DHCPv6 NFPF

- ND

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) (可选)

指定需要记录日志的端口 (可选)

GigabitEthernet 0/1

GigabitEthernet 0/2

GigabitEthernet 0/3

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 消息数/时间
100	1-4094	Gi0/1, Gi0/2, Gi0/3,	1000	1024/8640

33 NFPP

NFPP



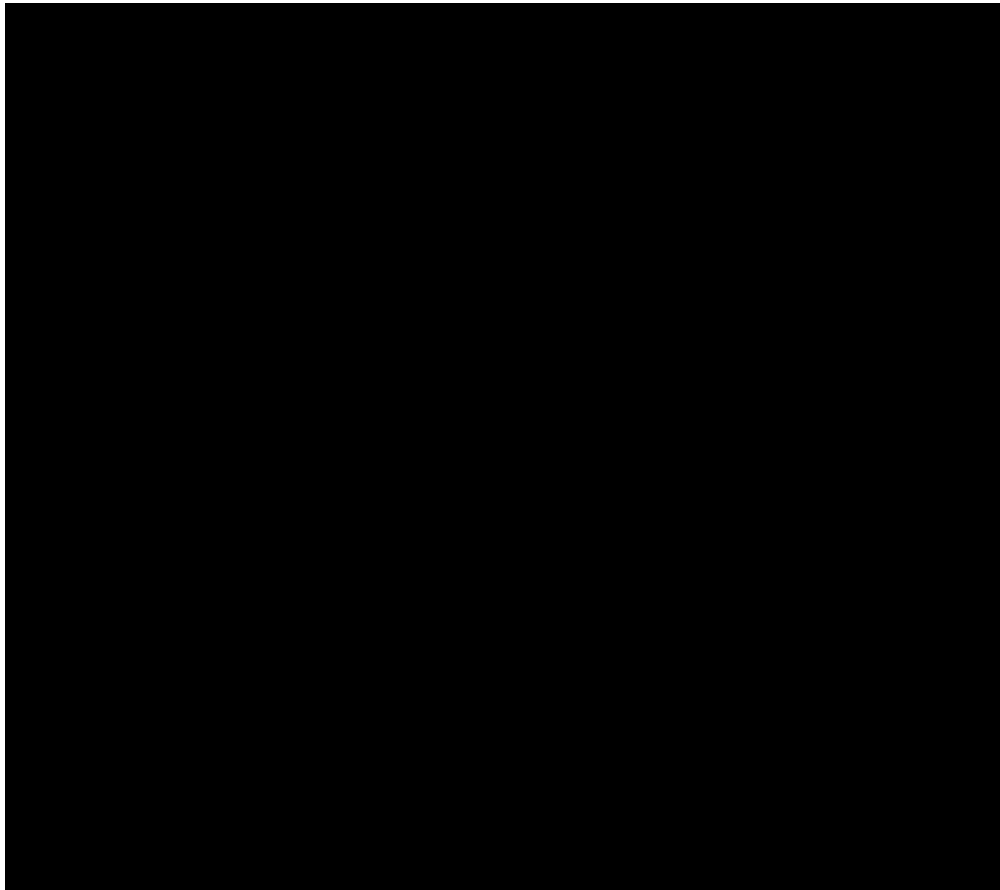
34

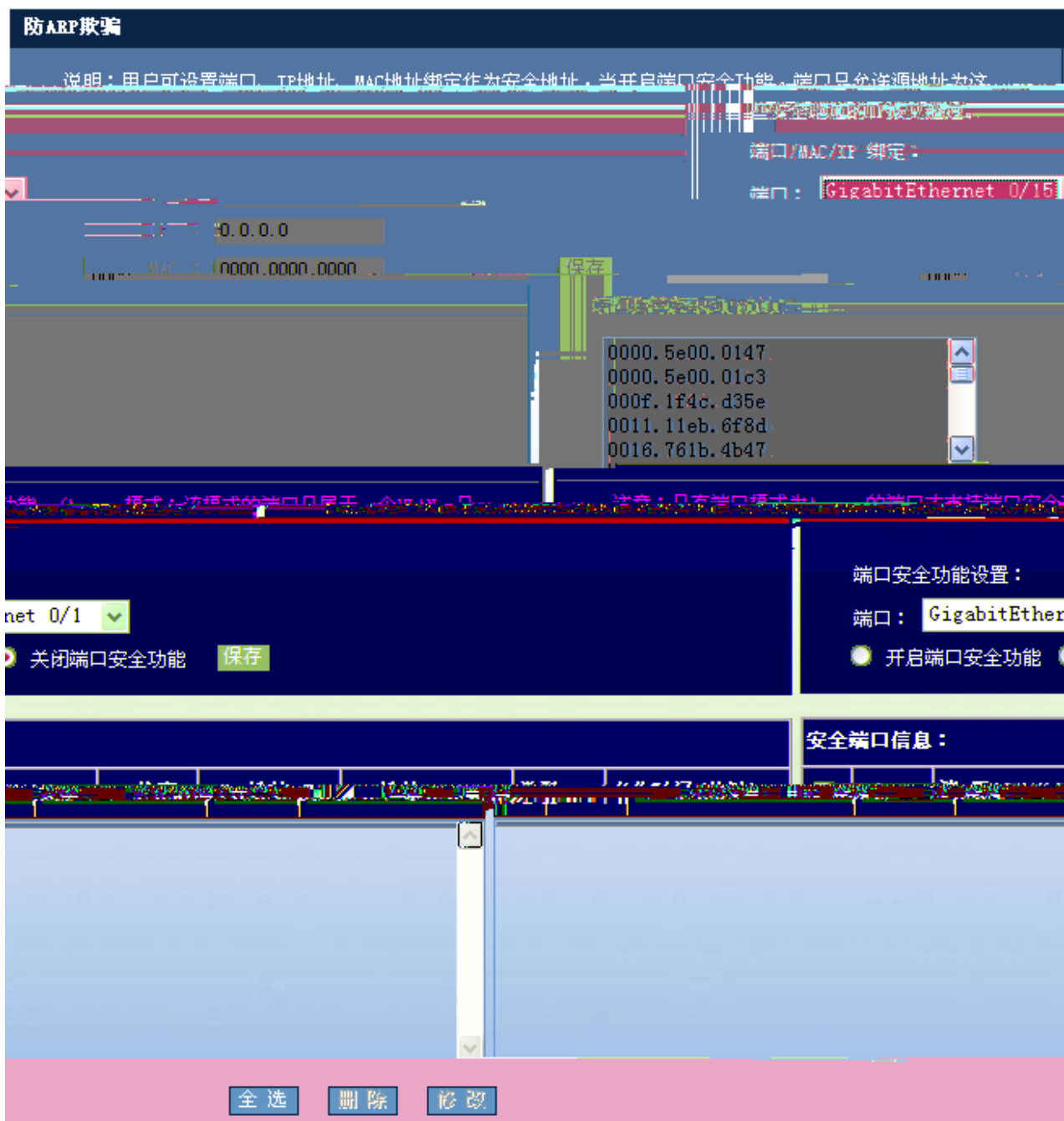
2.3

2.3.1 ARP

ARP

ARP





36 ARP

1) /MAC/IP

/MAC/IP

IP MAC

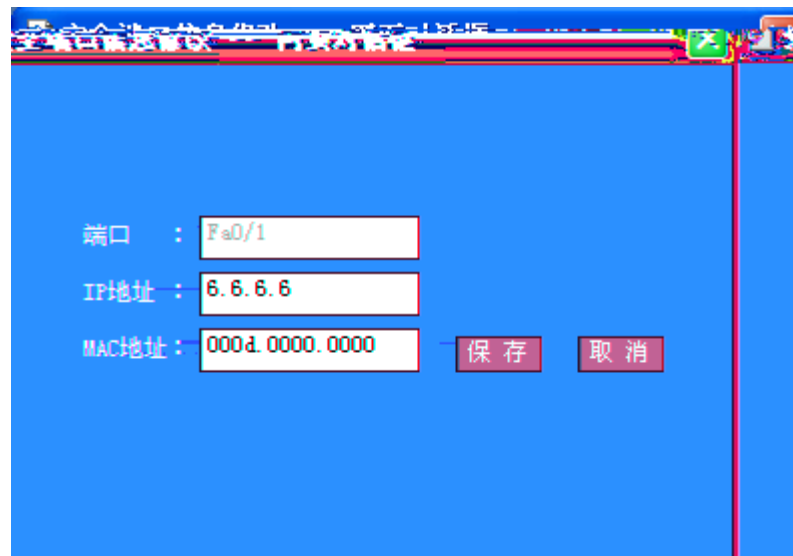
MAC

GigabitEthernet 0/15

MAC

2

3)



端口 : Fa0/1

IP地址 : 6.6.6.6

MAC地址 : 000d.0000.0000


保存 取消

37

2.3.3 APR

ARP

ARP



ARP检查设置

说明：ARP检查功能可以根据设置的安全地址对端口上收到的ARP报文进行检查过滤。

FastEthernet 0/1

开启ARP检查功能 关闭ARP检查功能 保存

38 ARP

ARP

ARP

2.3.4 ACL

ACL

ACL



39 ACL

1 ACL

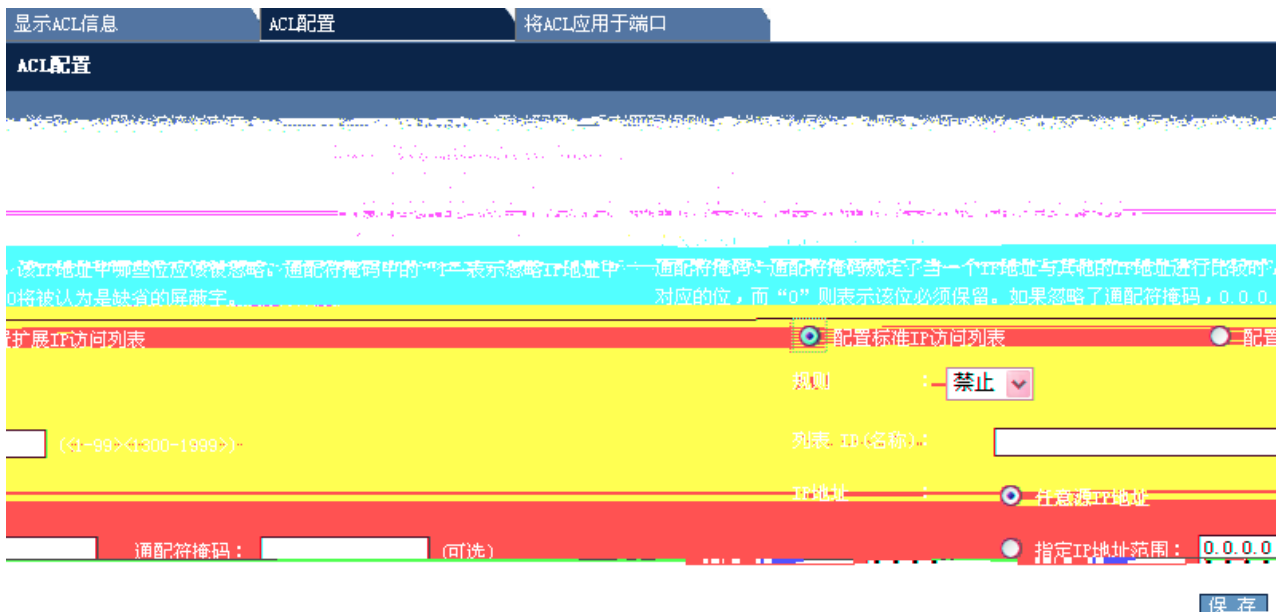
ACL
ACL

ACL ACE
ACL

ACL ACE
ACL

2 ACL
IP
IP

IP



40 IP

ID

IP

IP

,

IP

IP

IP

IP



41 IP

ID

TCP UDP IP ICMP

IP

IP

IP

IP

IP

IP

3 ACL

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

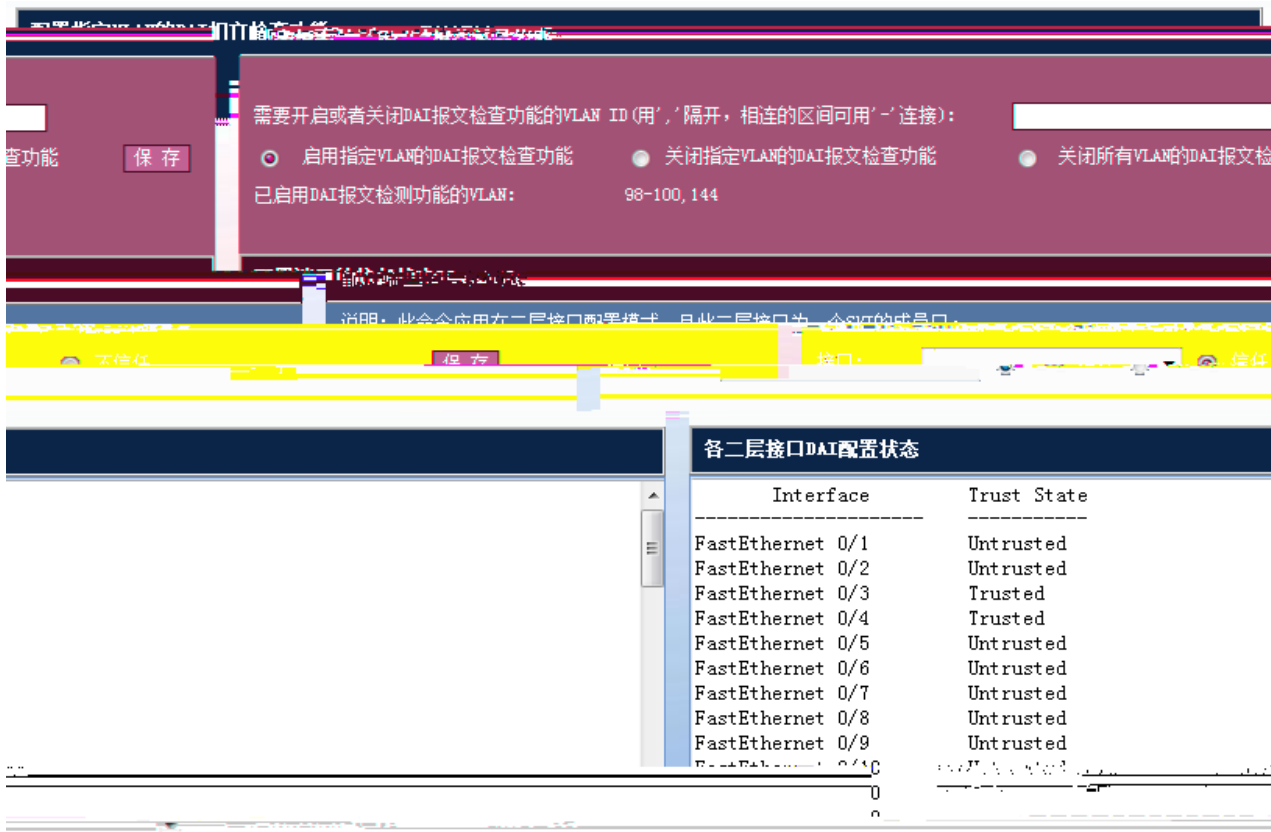
MAC MAC
 VLAN VLAN ID
 IP IP



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

DAI

2.3.7 CPP

CPP

配置报文的带宽和优先级

报文类型: [恢复默认配置](#)

带宽: (1-4096) [保存](#) 优先级: 0

[保存](#) [查看](#)

查看管理板/单机/堆叠系统的接收报文的统计信息: [查看](#)

查看线卡接收报文的统计信息: (2-8) [查看](#)

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	3

46 CPP

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

Radius服务器 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

非锐捷认证服务器动态acl下发: 开启 关闭

IP授权模式: disable 保存

Radius服务器组

组名:

正端口: (0-65536) (可选) UMF认证

帐端口: (0-65536) (可选) UMF记帐

保存

服务器组管理: radius 删除 刷新

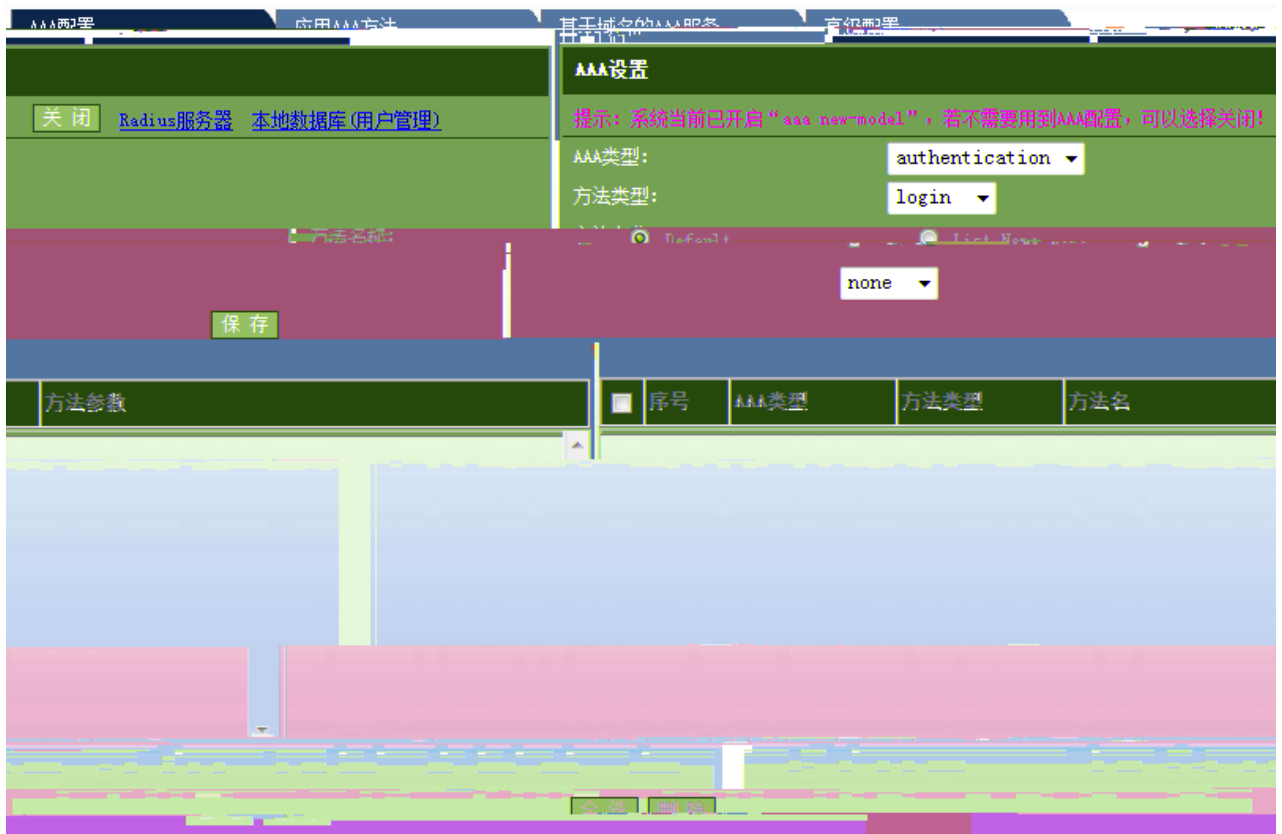
```

=====Radius group radius=====
Vrf:not-set
Server:7::1
  Authentication port:1812
  Accounting port:1813
  State:Active
Server:::1
  Authentication port:1812
  
```

192.168.1.100
port:1813
#

Vrf:not-set
Acc:using
State:Active

51 RADIUS



52 AAA

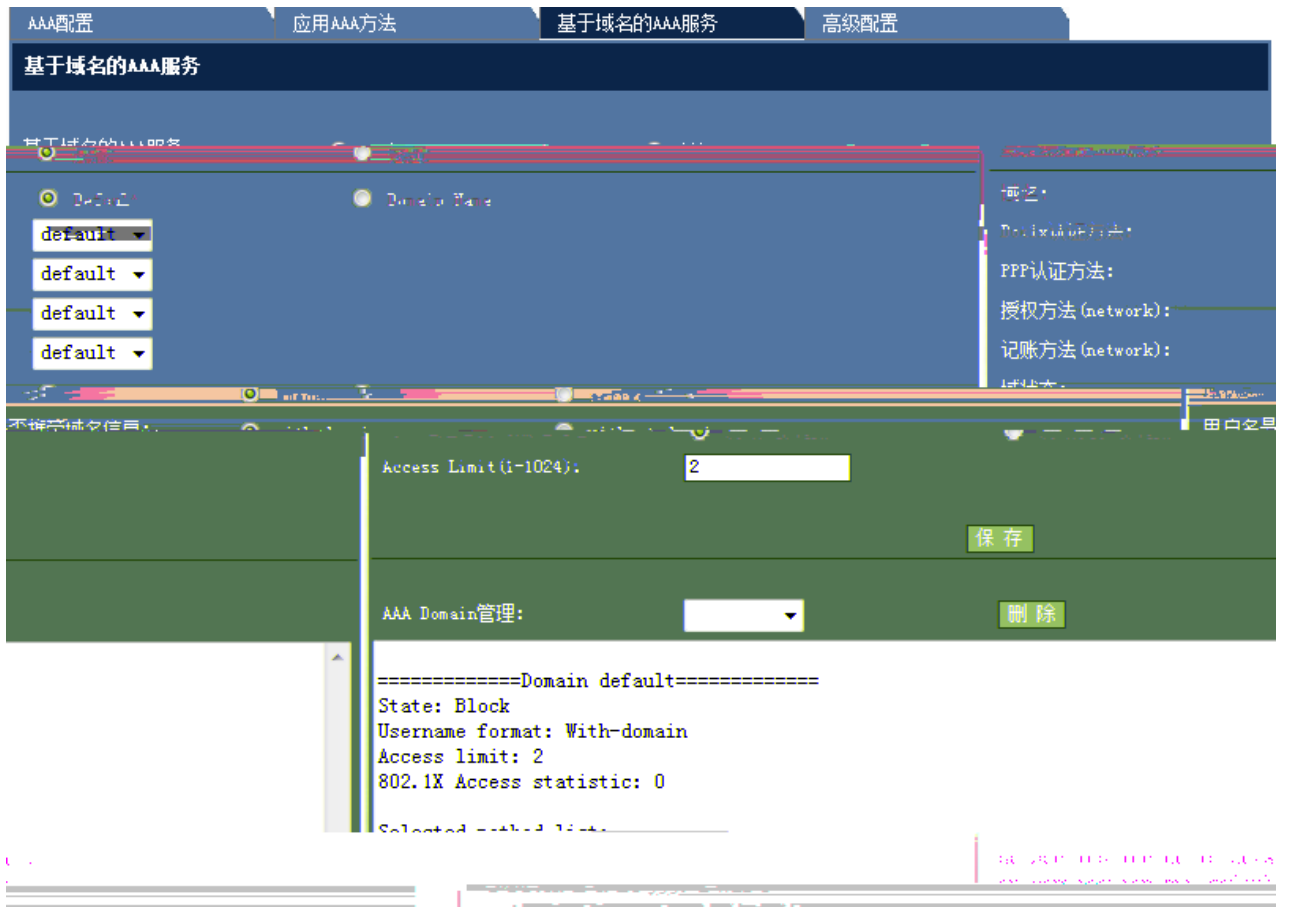
1

AAA

AAA

3

AAA



54

AAA

(network) AAA Dot1x PPP Access Limit

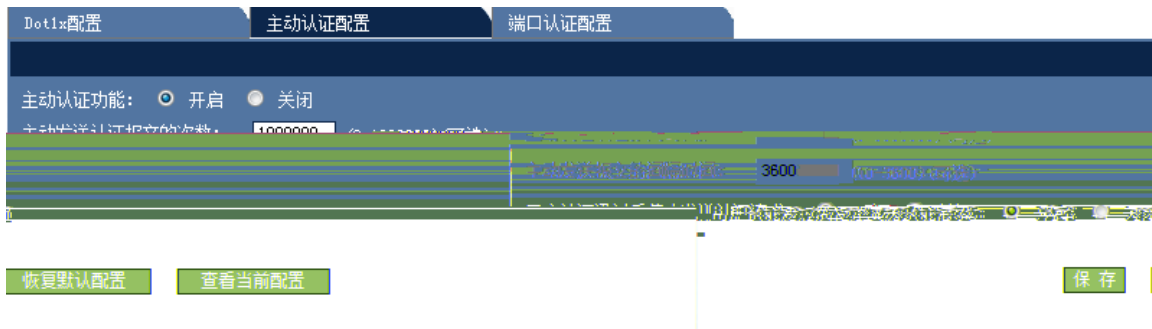
(network) (network)

AAA Domain

4 AAA

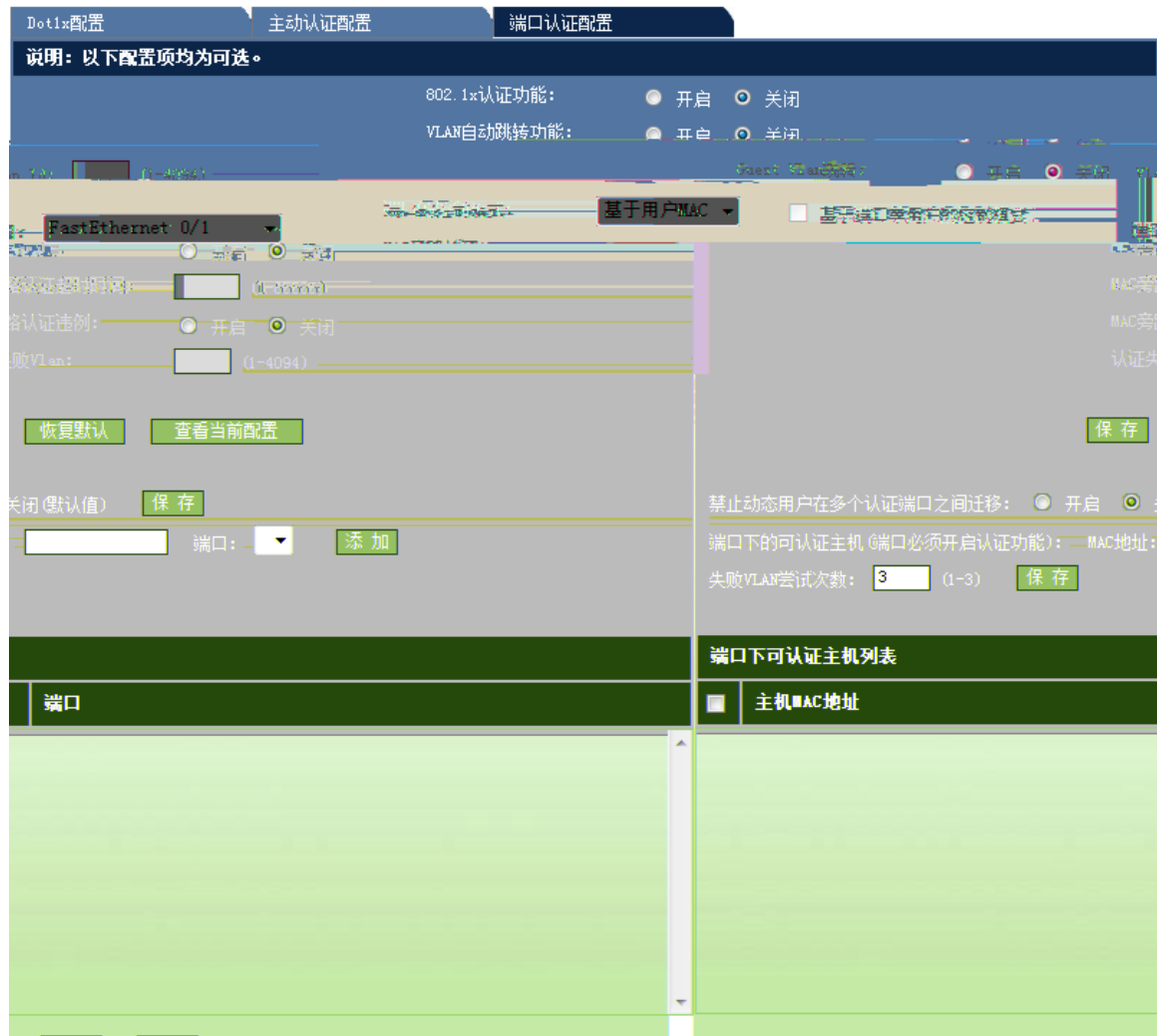
Dot1x

2



57

3



58

Dot1x

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.a805	1	绑定
3	192.168.23.55	0015.00.00.00	1	绑定
4	192.168.23.76	0015.00.00.00	5	绑定
5	192.168.23.76	0015.00.00.00	5	绑定
6	192.168.23.76	0015.00.00.00	5	绑定
7	192.168.23.76	0015.00.00.00	5	绑定

刷新

61 ARP

2.3.12 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

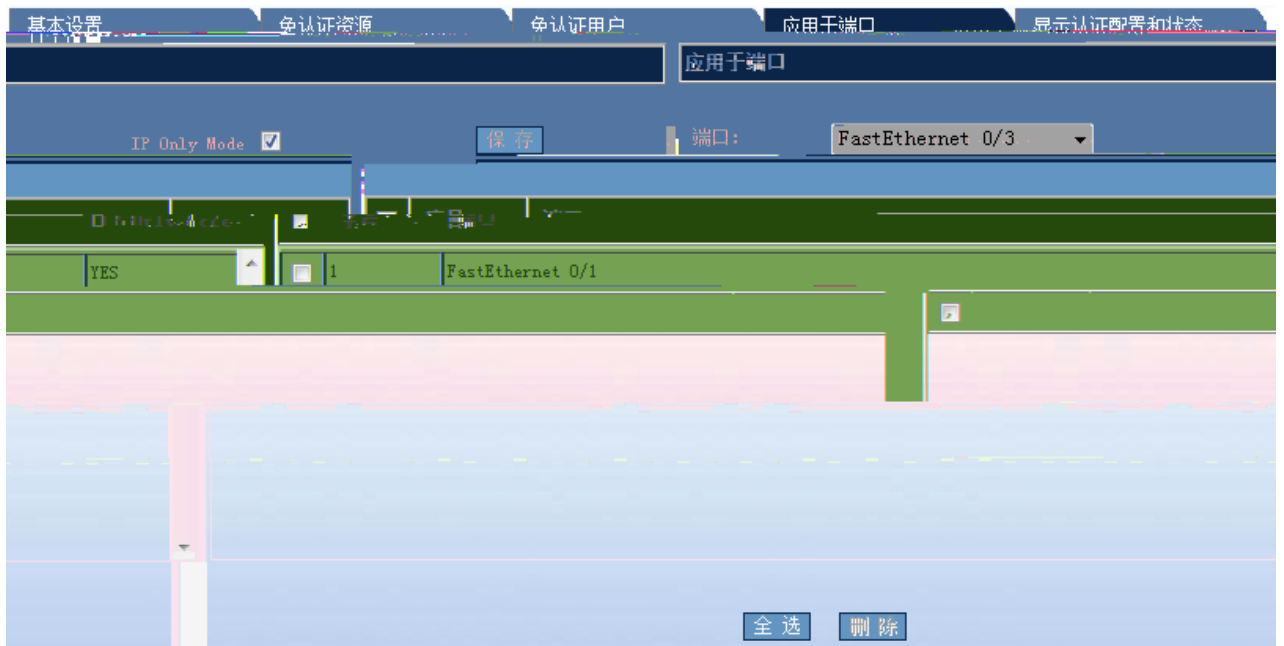
免认证的网络资源 (最多允许配置64个)

免认证的网络资源 (最多允许配置64个) 如果接入/汇聚设备启用了ARP、DHCP功能，那/需要对这些认证的网络资源进行ARP绑定，需要配置...

IP: 子网掩码 (可选): ARP

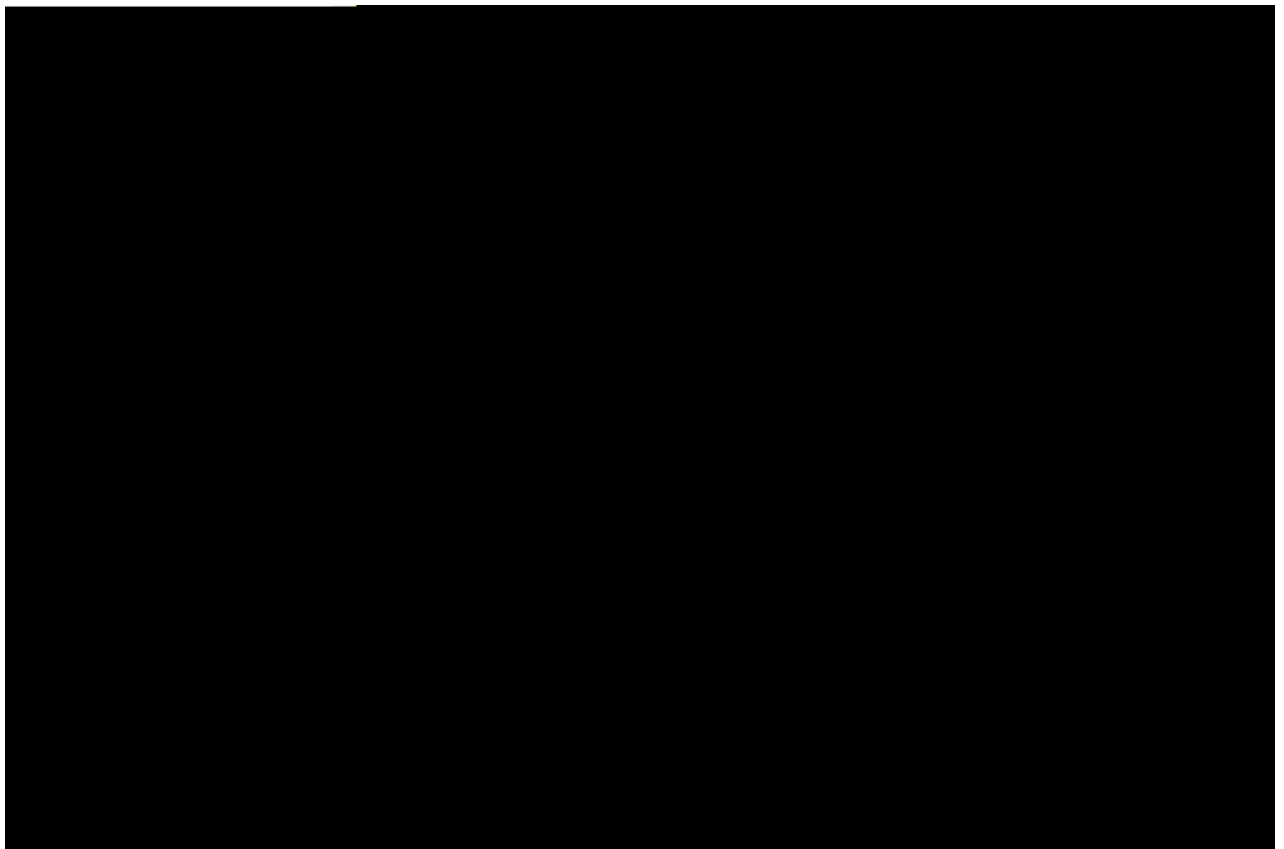
序号	IP地址	子网掩码	ARP绑定
1	1.2.3.6	255.255.255.0	Off

63.



65

5)



66

IP

2.3.13 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。

启用DHCP Snooping 禁用DHCP Snooping

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：

DHCP Snooping配置信息

	端口	信任端口	限速
1	FastEthernet 0/1	信任	

67 DHCP Snooping

2.4.4

将风暴控制应用于端口 (端口默认开启风暴控制)

端口: FastEthernet 0/2

广播 默认

单播

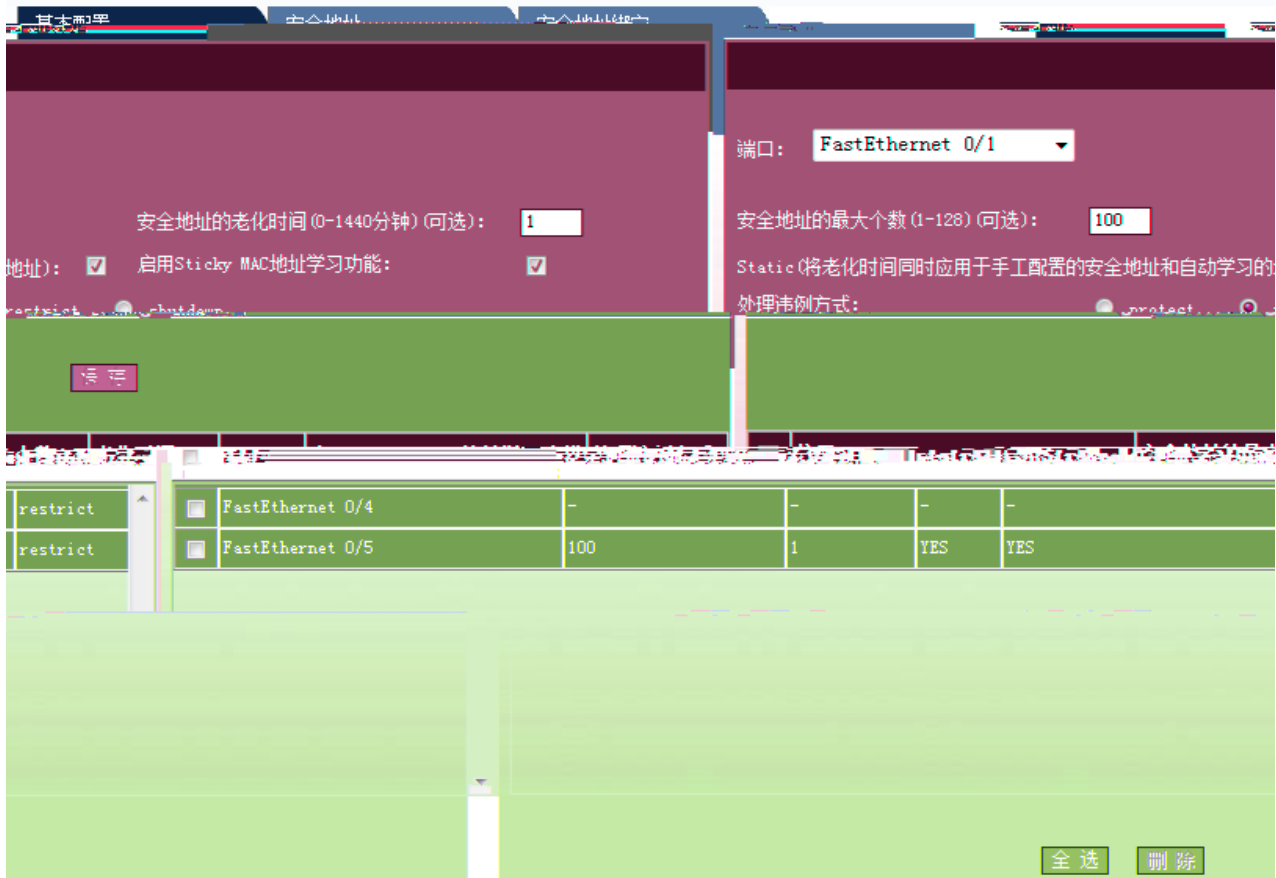
保存

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

全选 删除

71

2.4.5



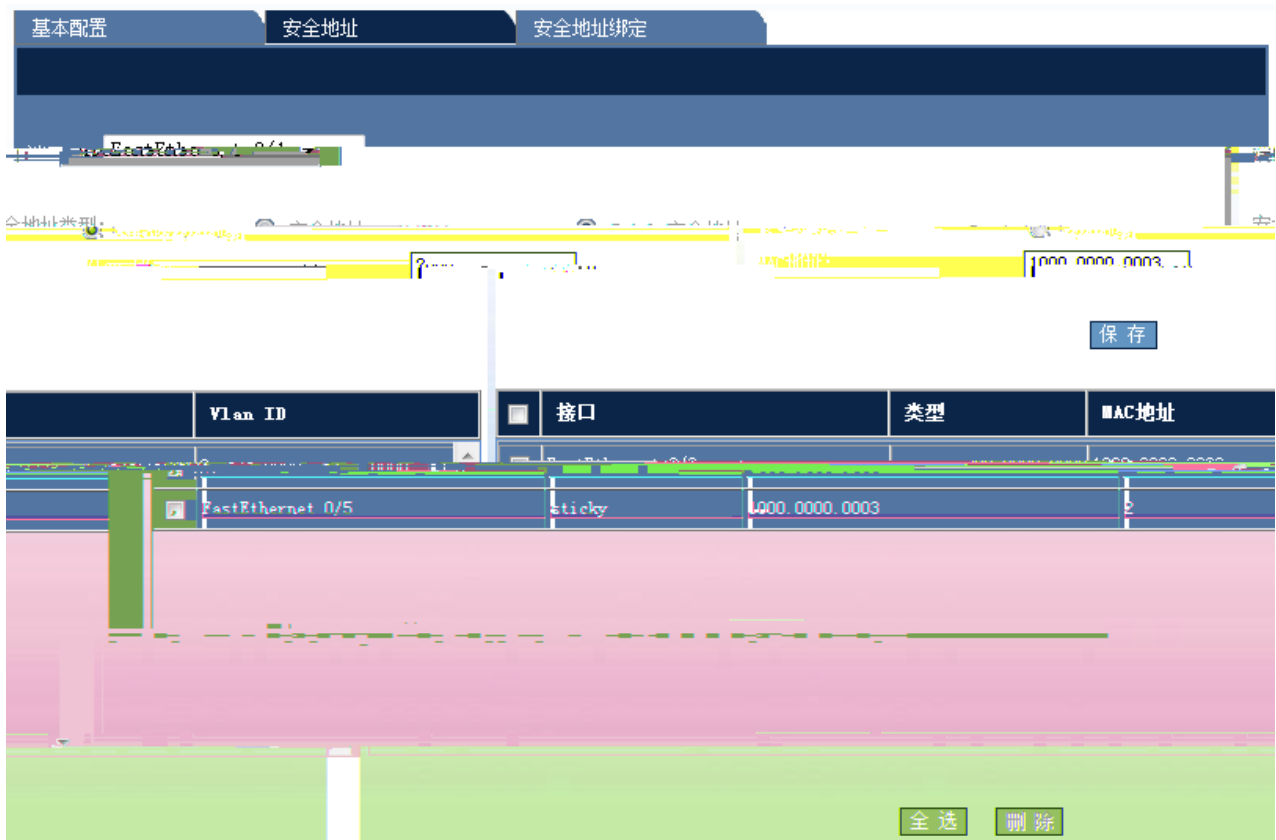
72

1)

Sticky Mac

Static

2)



73

Mac VLAN ID

3)

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

75

2.5.2

```

当前配置
Building configuration...
Current configuration : 12931 bytes

4      2008 -
        !
        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

```

76

2.5.3

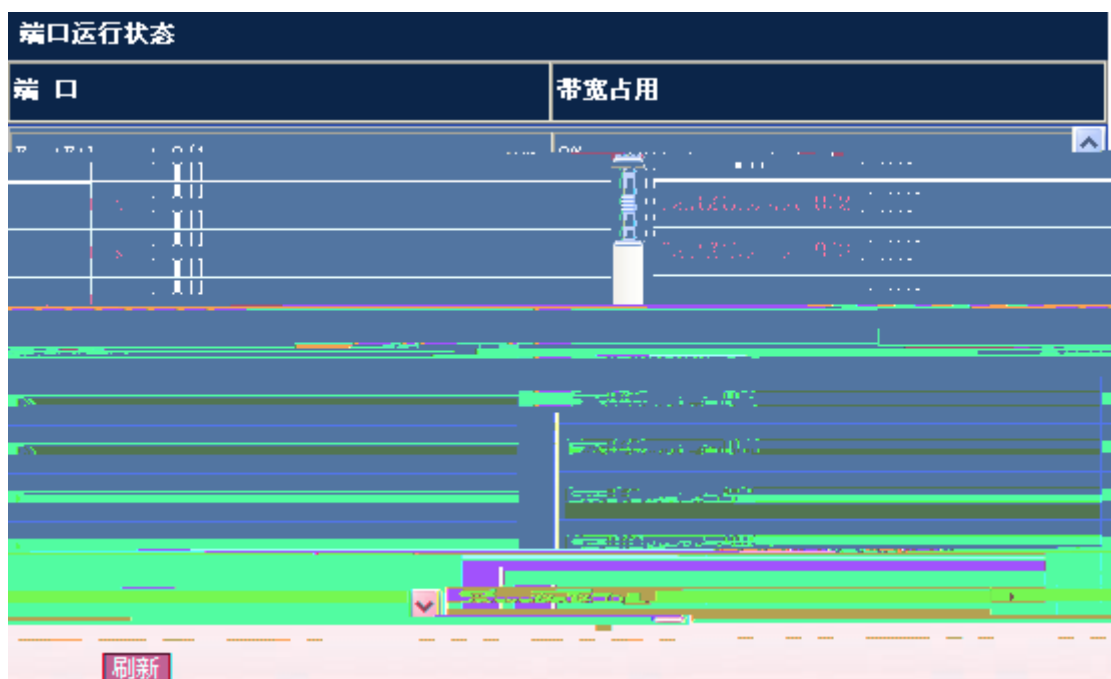
端口状态

端口	状态	速率	双工	介质	端口名称	
down	1	Unknown	Unknown	copper	FastEthernet 0/1	
down	2	Unknown	Unknown	copper	FastEthernet 0/2	
up	1	Full	100M	copper	FastEthernet 0/3	
down	900	Unknown	Unknown	copper	FastEthernet 0/4	
1	Unknown	Unknown	copper	FastEthernet 0/5	down	
1	Unknown	Unknown	copper	FastEthernet 0/6	down	
FastEthernet 0/10	down	1	Unknown	Unknown	copper	FastEthernet 0/10

刷新

77

2.5.4



78

2.5.5

1 : ...N© 1 5 AÁS2µ DM' Ö

端口统计信息

注意：选择 All Ports 时，将显示所有端口的统计信息。

清零 端口：

输入/输出板统计

接收广播包数	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
8740	14043	12012	343	1588	Gi0/1	33198	8950	5508	11
0	0	0	0	0	Gi0/2	0	0	0	0
3	2717	0	0	6	Gi0/3	2157	2146	5	54
0	0	0	0	0	Gi0/4	0	0	0	0
175	0	0	0	11	Gi0/5	34	23	0	27
0	0	0	0	0	Gi0/6	0	0	0	0
5541	2298818	0	0	69848	Gi0/7	882792	404167	408777	68
0	0	0	0	0	Gi0/8	0	0	0	0
1269	842417	0	0	37	Gi0/9	437082	435647	1398	19
0	0	0	0	0	Gi0/10	0	0	0	0
4472	2367132	0	0	149	Gi0/11	856226	850552	5525	75
0	0	0	0	0	Gi0/12	0	0	0	0
0	0	0	0	0	Gi0/13	0	0	0	0
0	0	0	0	0	Gi0/14	0	0	0	0
3	8386	0	0	935630	Gi0/15	5557815	1423231	3198954	21
0	0	0	0	0	Gi0/16	0	0	0	0

刷新

79

2.5.6

```

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
*****SequenceNumber Log Messages: disable*****
Sysname log messages: disable
Count log messages: disable
Trap logging: level informational, 587 message lines logged, 0 fail
Log Buffer (Total 4096 Bytes): have written 4096. Overwritten 2533
*Feb 28 08:20:45: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 08:33:51: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 08:43:52: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 08:53:54: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 09:03:55: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 09:13:56: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 09:23:57: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 09:33:58: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 09:43:59: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 09:54:00: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 10:04:01: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 10:14:02: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 10:24:03: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 10:34:04: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 10:44:05: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 10:54:06: %ARPGUARD-4-SCAN: ARP scan was detected.

```

80

2.6

2.6.1 Ping

Ping

IP

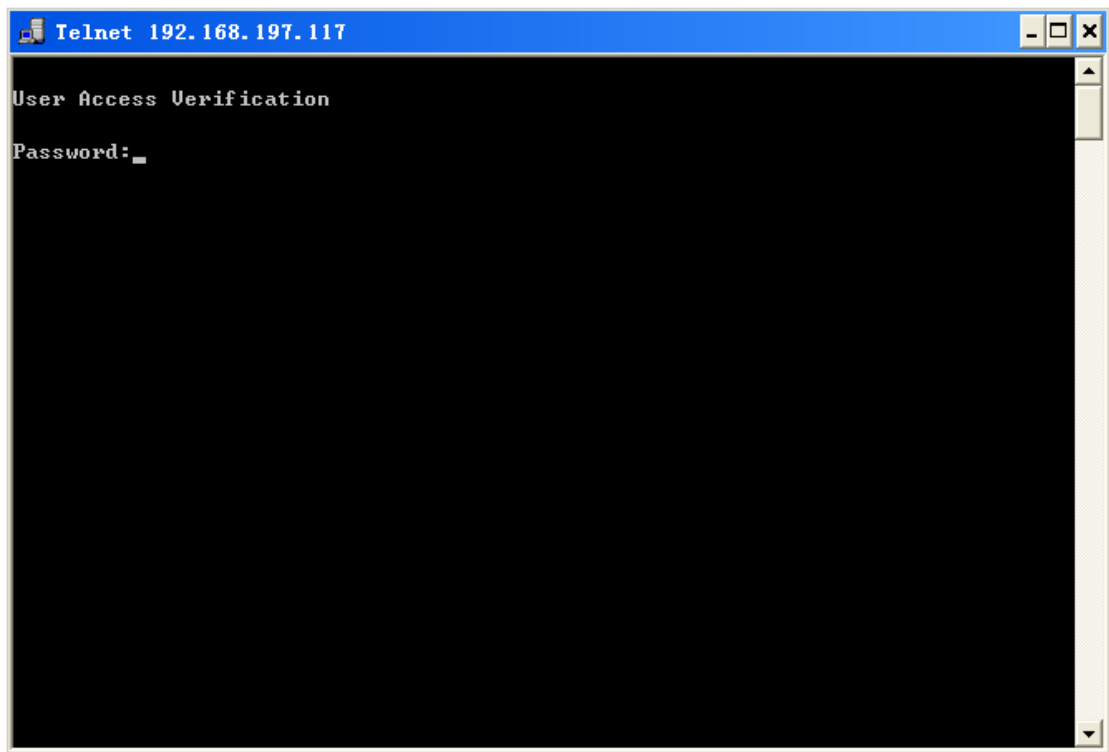
IP

Ping

2.6.2 Telnet

Telnet

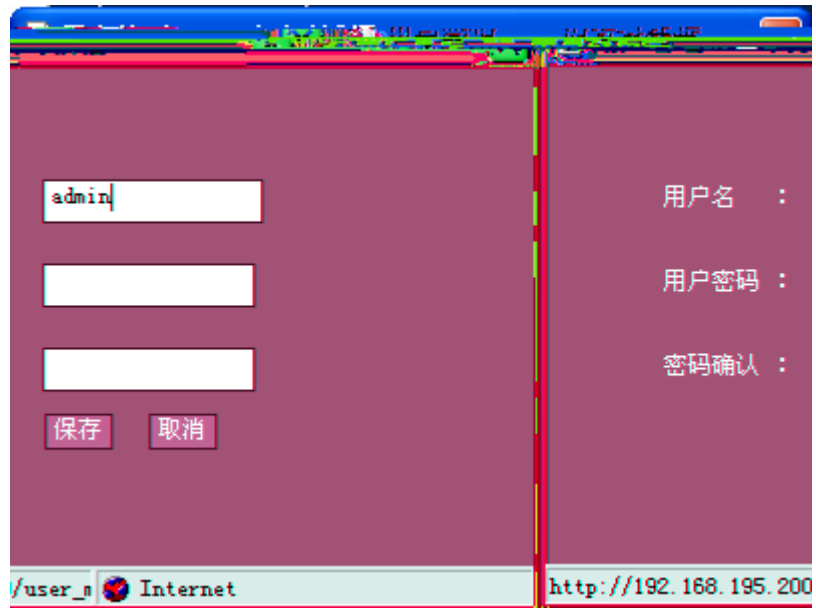
Telnet



82 Telnet

PC Telnet Telnet PC Telnet

2.6.3



85

2.6.4

修改Enable口令

Enable口令，则在设置之后使用新口令重新登录。

注意：如果您设置了新的

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

86

- 1) Enable
Enable



87

- 2) Telnet
Telnet

8080

IP

192.168.1.1

:8080

2.6.7

系统升级

注意：请确认TFTP服务器已启用！

源文件名：

目标文件名：

TFTP 服务器 IP：

文件传输信息：

系统升级过程需要若干分钟,请耐心等待...

90

TFTP



