



©2015



RGOS 10.4 (2b12)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



1)

[] []

{x | y | ... }

[x | y | ...]

//

2)

3)

1 WEB

WEB

IE

WEB

WEB

WEB

WEB

2 WEB

2.1

WEB

WEB	

WEB	“ WEB ”
WEB Enable	
Enable	

IP _____,



1

WEB enable	Enable
---------------	--------

2.2

2.2.1 IP

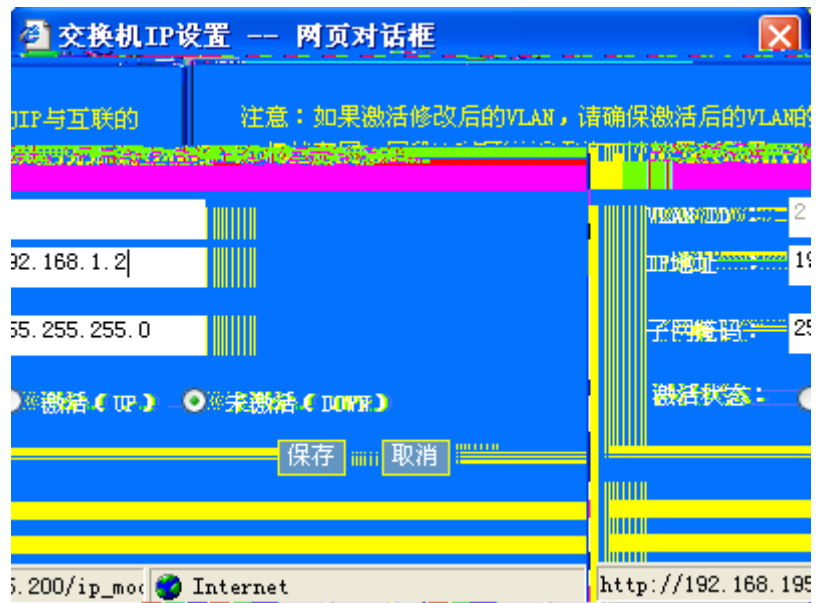
" IP "

IP



4 IP

ip " "



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，通过配置交换机，将网络划分为多个逻辑子网，使得同一子网内的用户可以进行二层通讯。

名称	状态	<input type="checkbox"/>	VLAN ID	VLAN
001	STATIC	<input type="checkbox"/>	1	VLAN0
002	STATIC	<input type="checkbox"/>	2	VLAN0

新建 全选 删除 修改

6 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

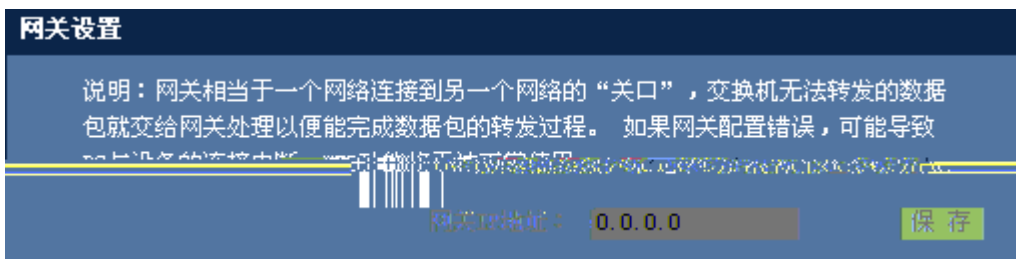
9 VLAN

VLAN ID

" "

2.2.3

" "



10

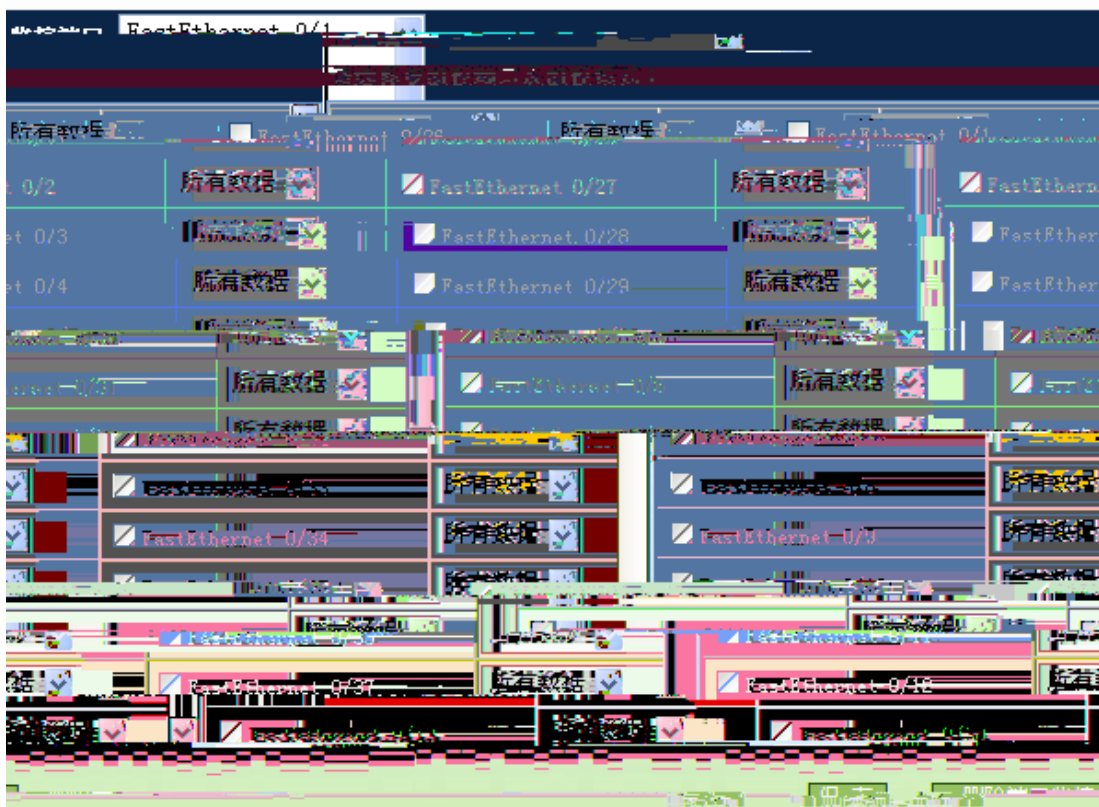
IP

IP

" "

2.2.4

" "



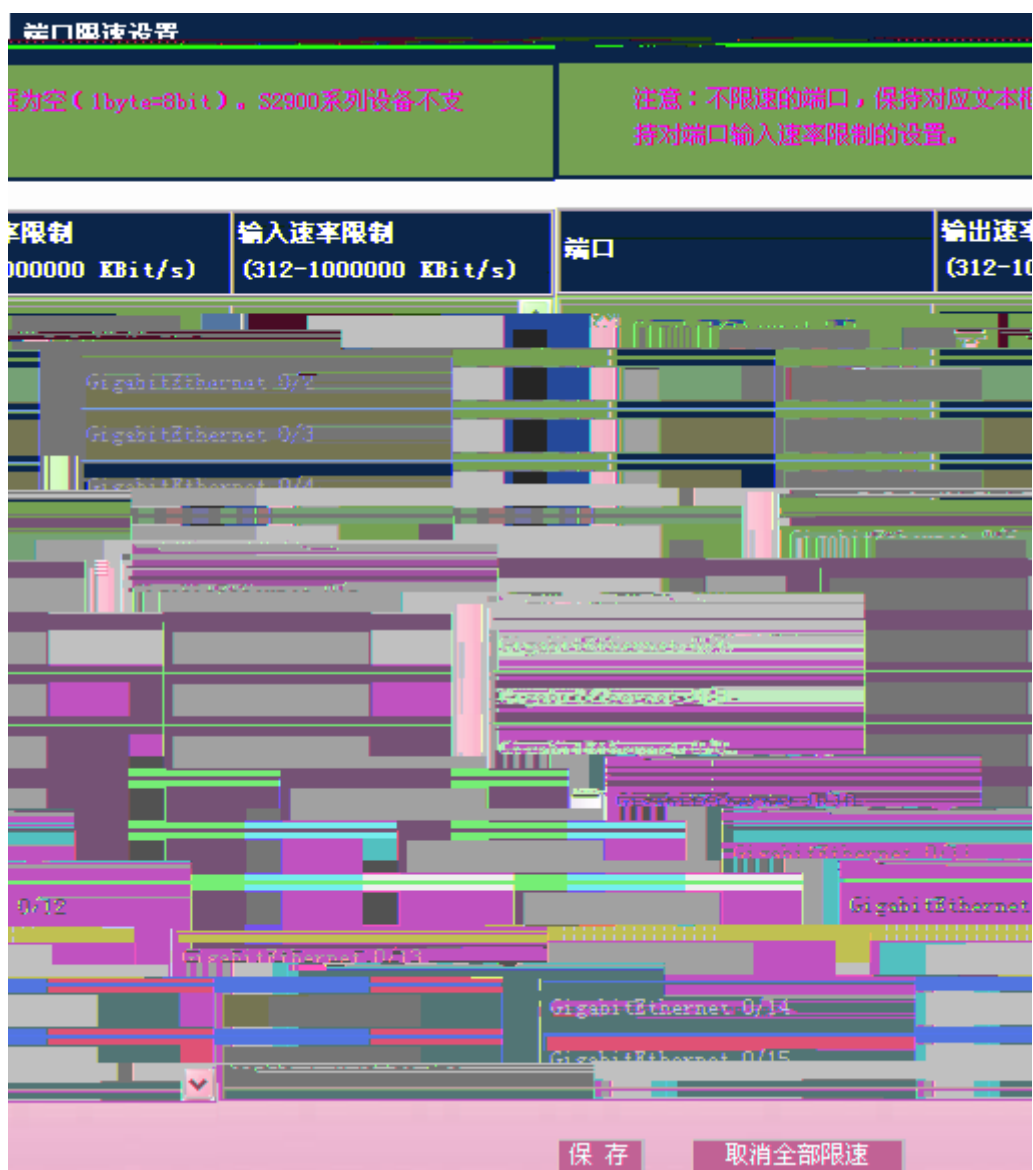
11

" "

" "

2.2.5

" "



12

" "

" "

2.2.6

" "



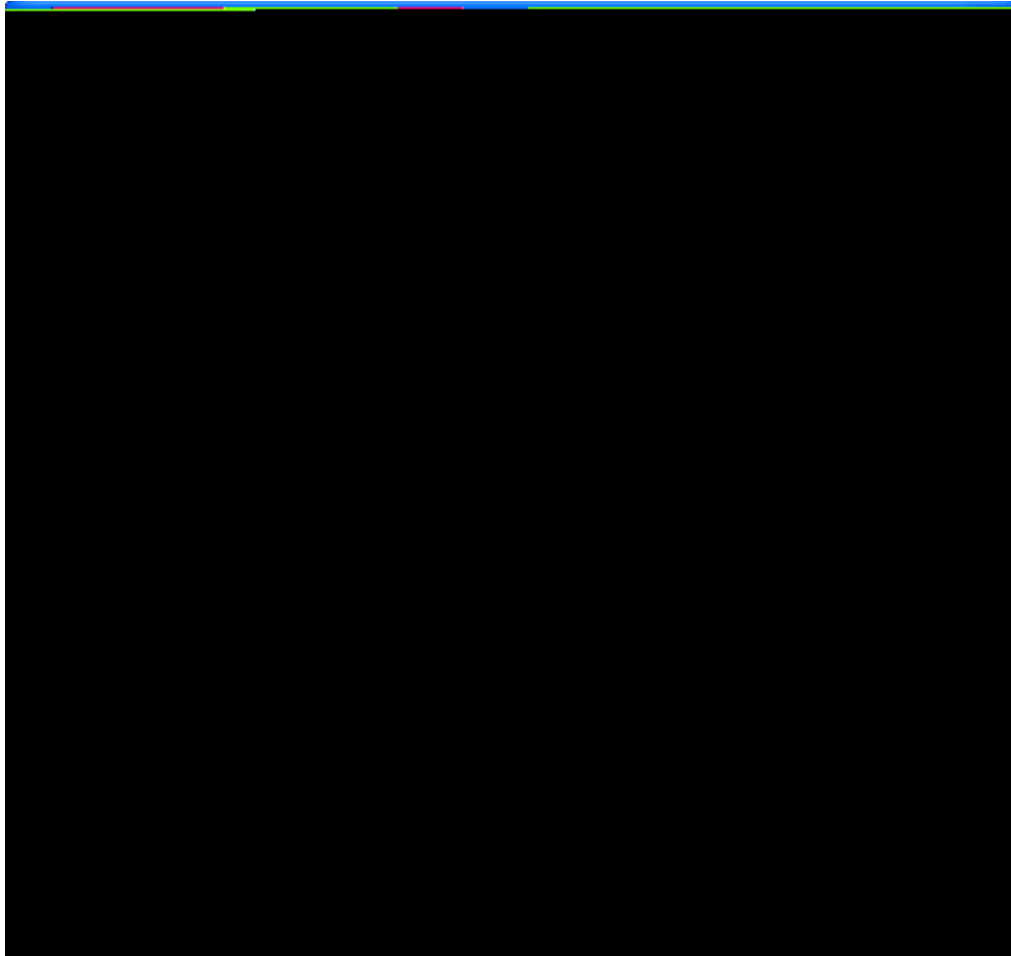
13

1

" "

2

" "



14

" "

3

" "

2.2.7

" "



16 DHCP

1) / DHCP

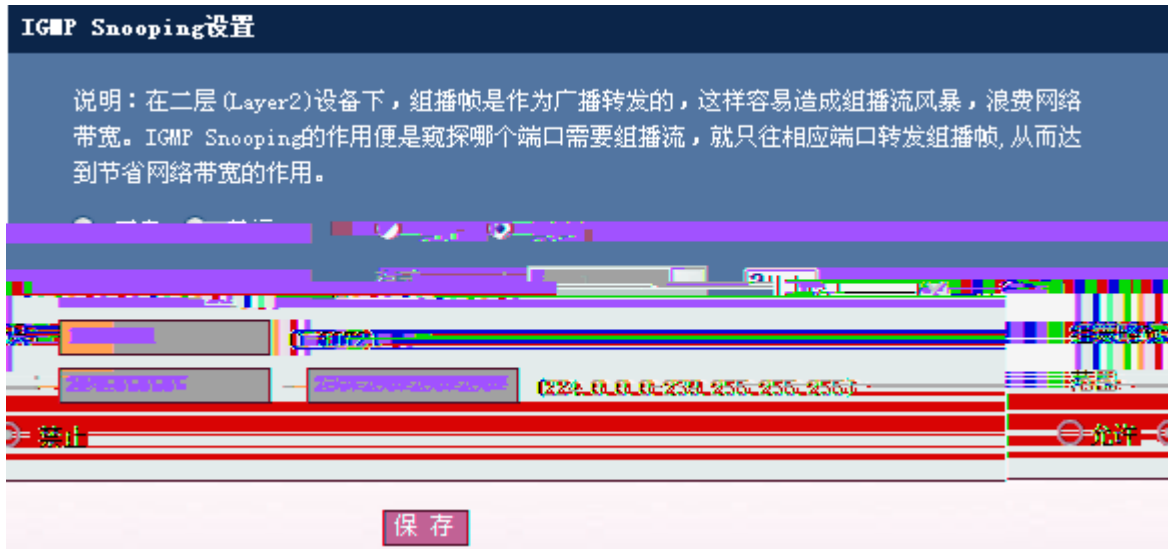
/ DHCP " "

2) DHCP

DHCP " "

DHCP " "

" C



17 IGMP Snooping

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

2.2.10 STP

" STP

SNMP



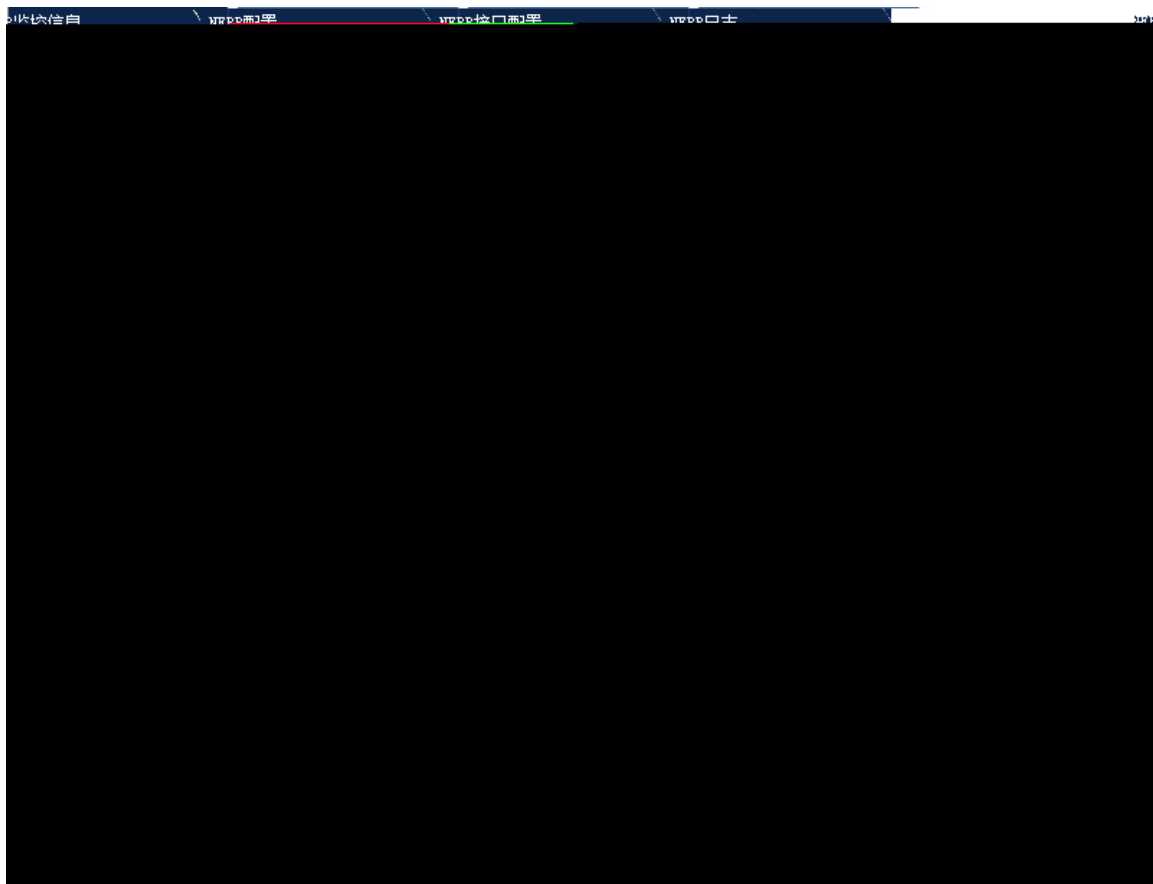
19 SNMP

SNMP " SNMP"

" " " "

" SNMP" " "

" "



20 NFPP

ARP

www.检测信息 www.配置 www.检测信息 www.日志

NTPP监控信息查看与配置

查看全部:

(可选) VLAN (1-4094) (可选) 端口 (可选) MAC

查看全部:

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

ARP扫描表信息		ARP扫描表信息		
MAC address	timestamp	VLAN	interface	IP address
001a.a942.f27f	2016-6-6 11:8:53	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:10:1	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:10:2	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:10:3	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:10:4	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:10:5	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:11:0	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:11:1	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:11:2	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:12:2	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:13:3	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:14:4	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:15:4	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:16:5	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:17:13	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:18:14	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:19:15	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:20:23	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:21:24	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:22:24	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:23:25	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:24:26	1	Fa0/40	-
001a.a942.f27f	2016-6-6 11:25:34	1	Fa0/40	-

21 ARP

ARP

"

ARP

"

ARP

"

ARP

"

ARP

"

ARP

"

"

"

"

"

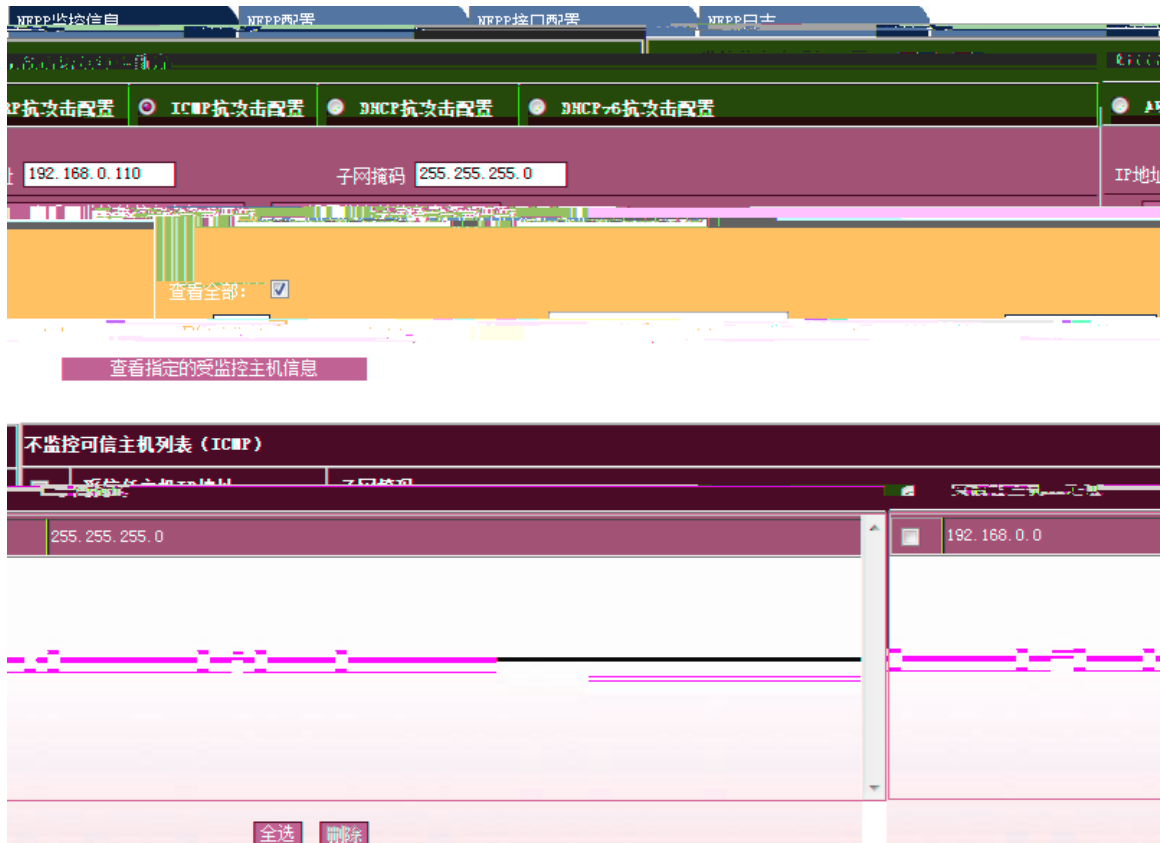
"

"

"

"

ICMP



22 NFPP

--ICMP

ICMP

"

"

IP

"

"

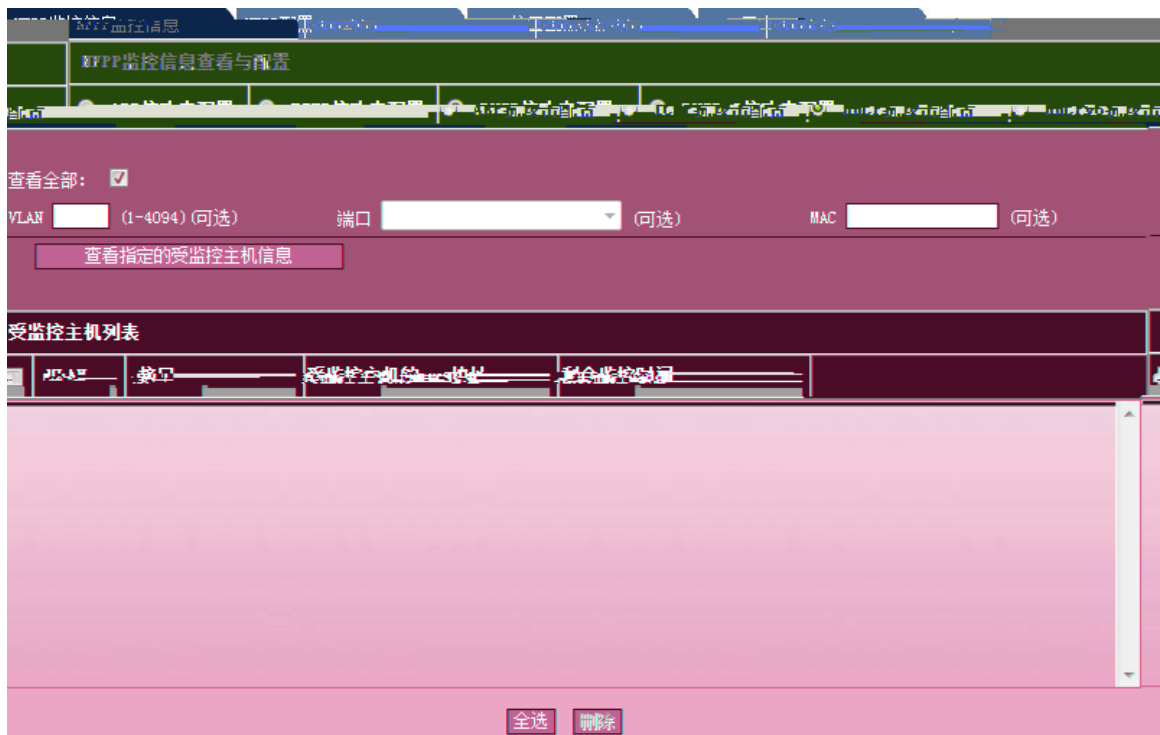
"

"

"

"

DHCP



23 NFPP

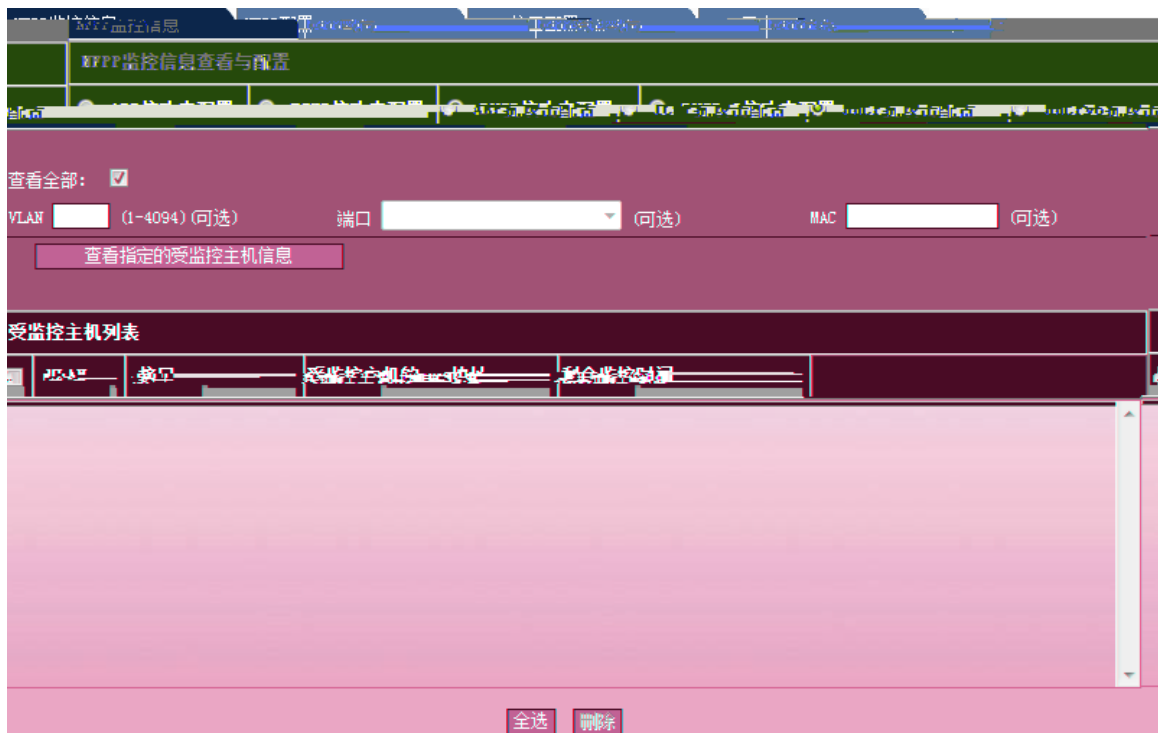
DHCP

DHCP

" " " "

" "

DHCPv6



24 NFPP

DHCP

DHCPv6

"



25 NFPF
CPU

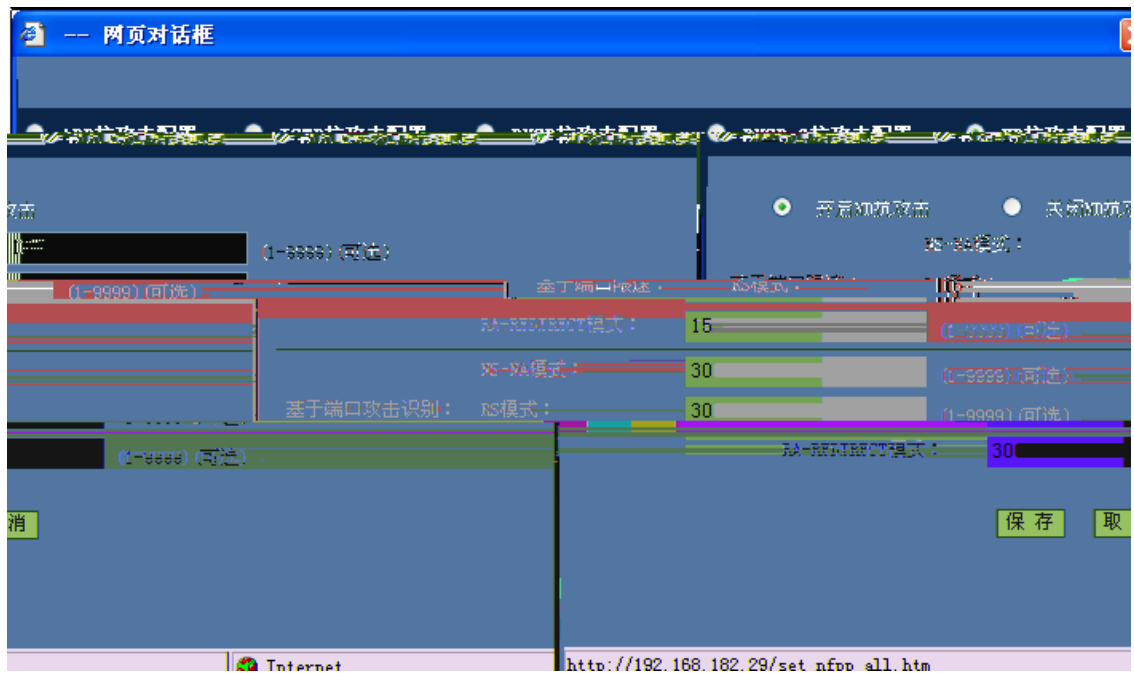
DHCPv6



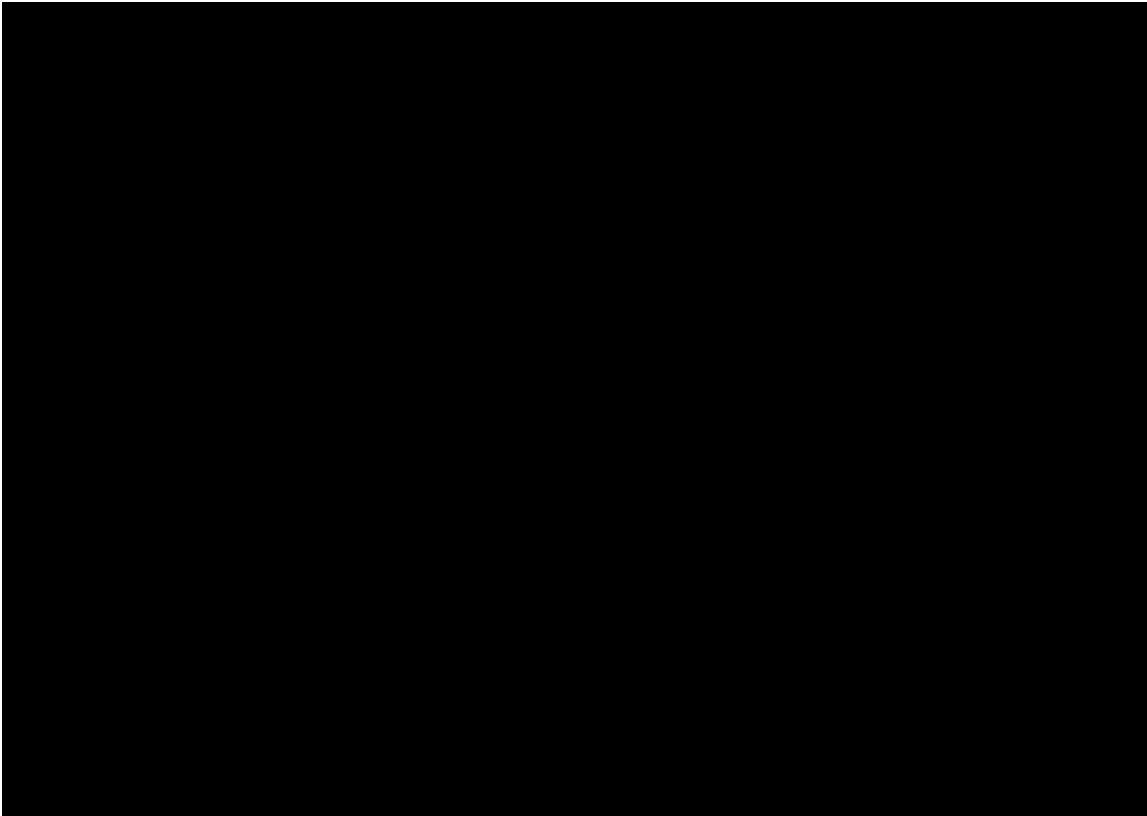
26 CPU

CPU

NFPF



27 NFPP



28 NFPP NFPP ARP

ARP NFPP

“ ”

ICMP



29 NFPP NFPP ICMP

ICMP NFPP
" "

DHCP



30 NFPP

NFPP

DHCP

DHCP

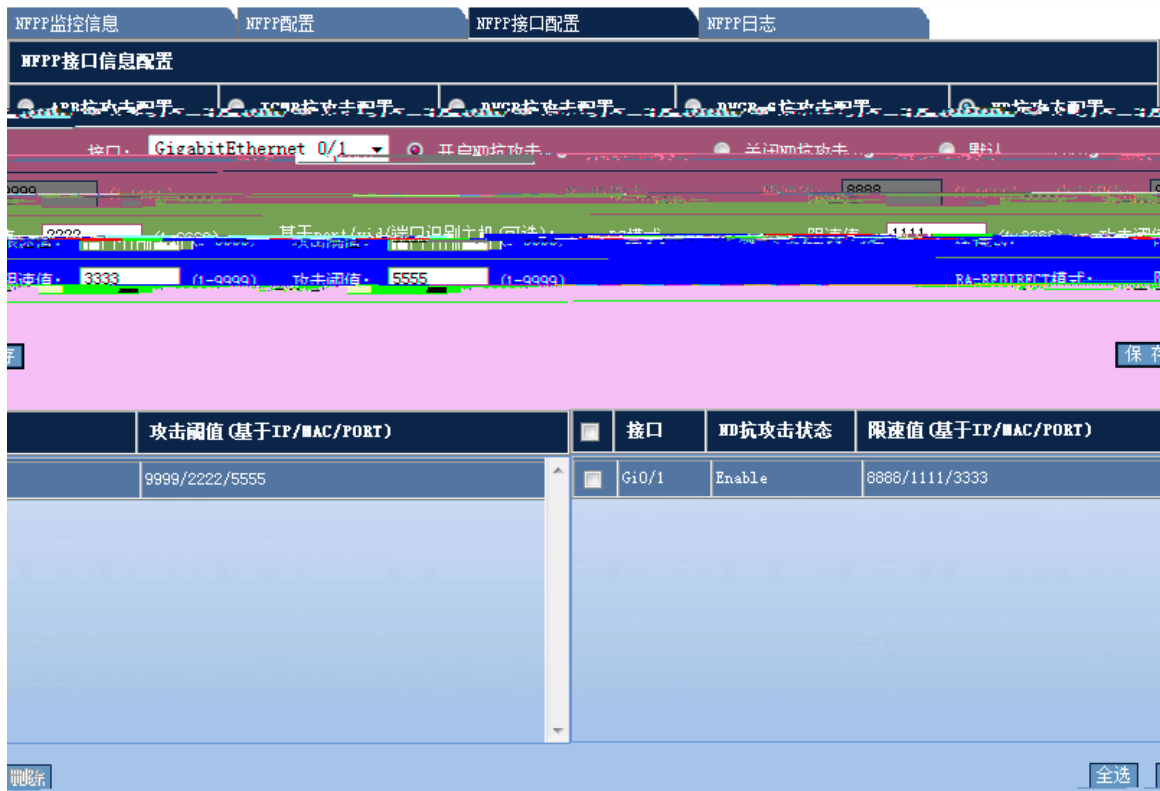
NFPP

"

"

DHCPv6





32 NFPP

NFPP

ND

ND

NFPP

"

"

4 NFPP



33 NFPP

NFPP

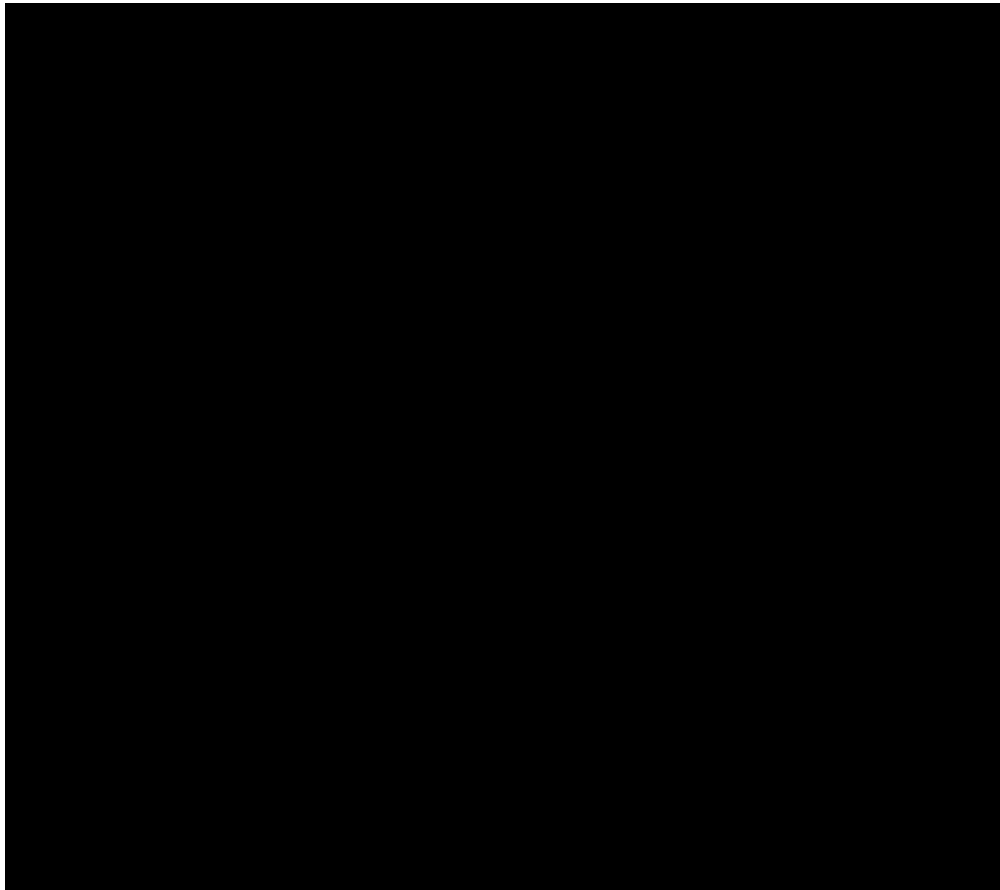
" "

"

"

"

"



35 ARP

" "

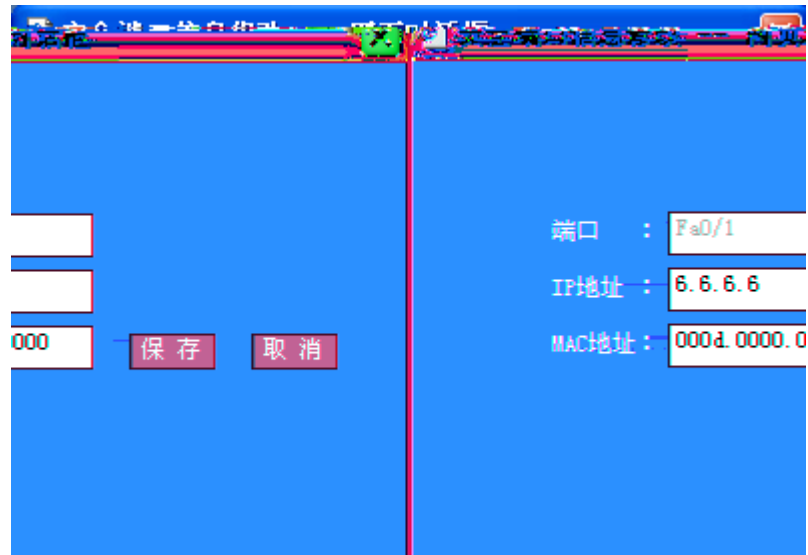
" "

2.3.2 ARP

" ARP "

ARP

3)

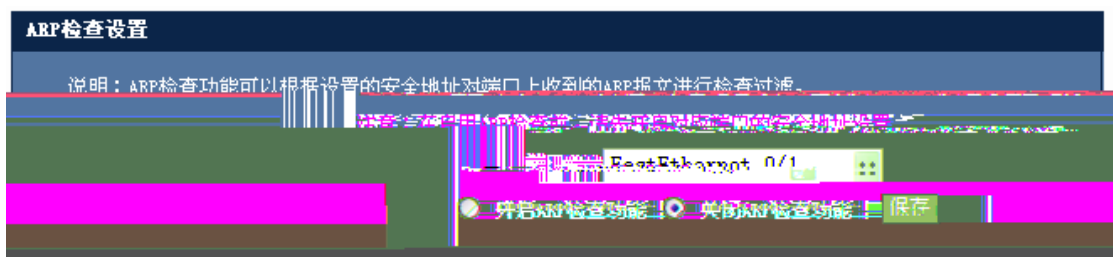


37

2.3.3 APR

" ARP "

ARP



38 ARP

" ARP "

2.3.4 ACL

" ACL "

ACL



39 ACL

1 ACL

ACL

ACL

ACE " " " "

ACL

ACL

ACE

ACL " "

ACL

ACE

2 ACL

IP

"

IP

"

IP

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）

编号为1 - 99，1300 - 1999

对每一位，前“0”则表示该位必须保留。如果忽略了通配符掩码，0.0.0.0将被认为是缺省的掩码字。

ACL 禁止

协议：TCP

源IP地址：0.0.0.0

源端口：任意

目的IP地址： 任意目的IP地址

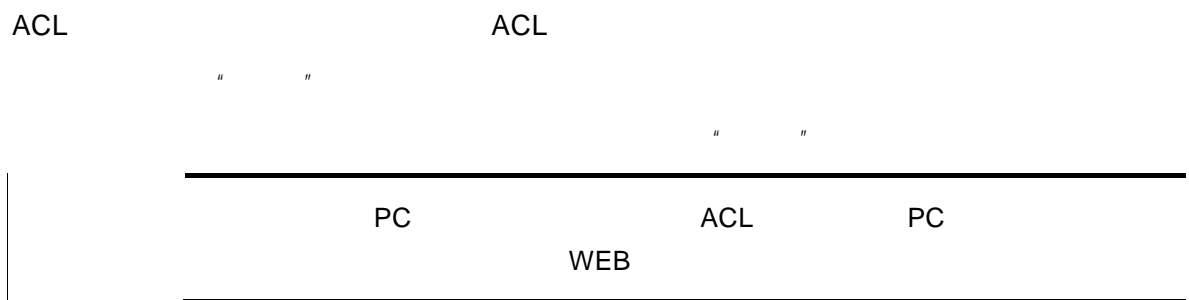
目的端口： 0.0.0.0 通配符掩码

保存

41 IP

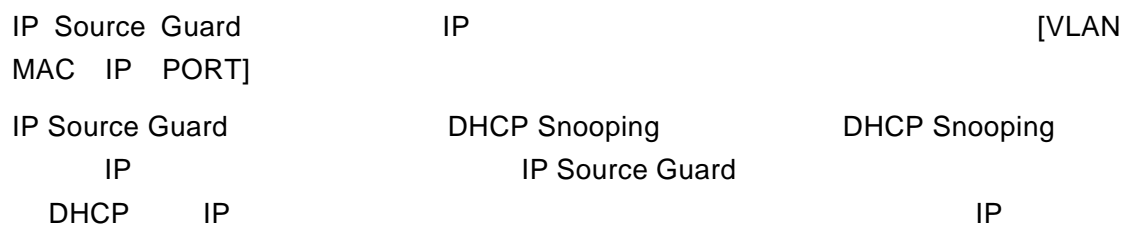


42 ACL



2.3.5 IP Source Guard

IP Source Guard:



IP Source Guard DHCP Snooping
DHCP Snooping

" IP Source Guard"

IP Source Guard



43 IP Source Guard

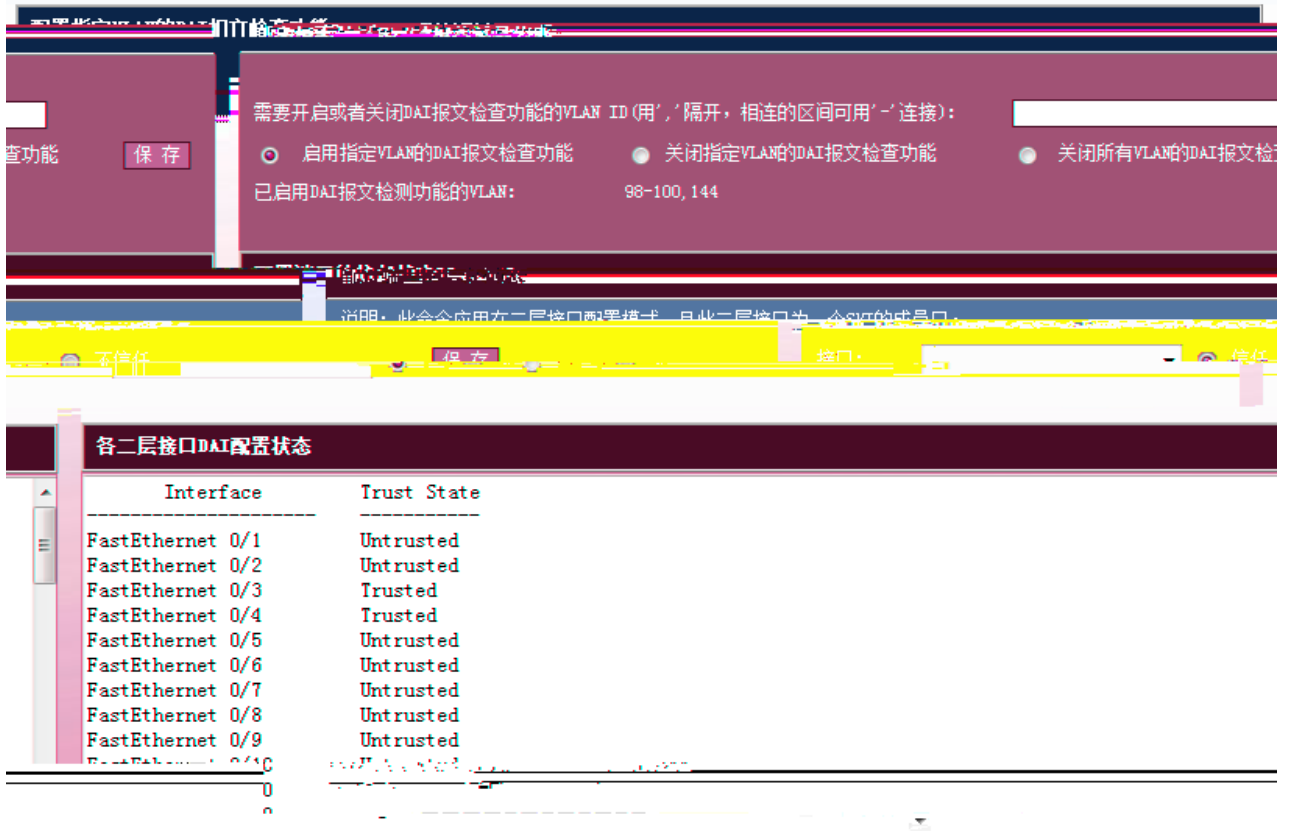
1

IP Source Guard

IP+MAC " IP+MAC ()"

2

IP



45 DAI

```

1          VLAN  DAI
          VLAN  DAI
          VLAN 100  DAI          vlan-id  100  ARP          DAI

"          DAI          VLAN ID"          VLAN
          VLAN  DAI
          DAI          VLAN

2          ARP
          DAI          ARP          ARP
          DAI
  
```

" " " "

3)

GSN

GSN

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
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

49

/ /

" "

/ /

Radius服务器 Radius服务器组

AAA参数配置

AAA new-model: 开启 关闭

密钥:

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

Radius服务器

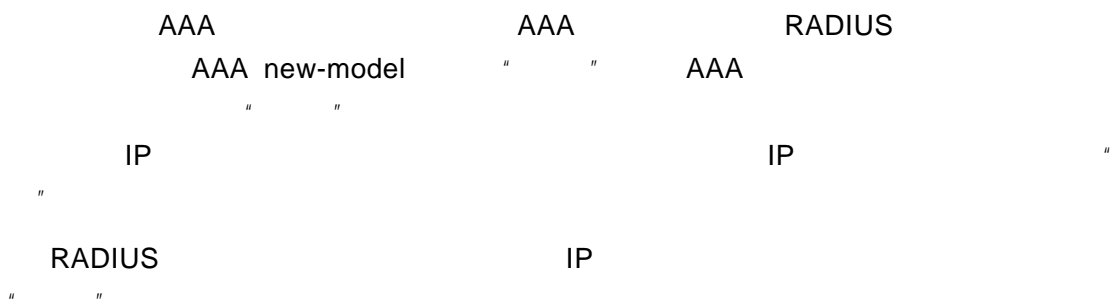
Radius服务器IP地址:

UDP认证端口: (0-65535) (可选)

UDP记账端口: (0-65535) (可选)

认证端口	记账端口	服务器状态	Radius服务器IP地址	认证
13	1812		192.168.0.111	18

51 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

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) UDP认证

帐端口: (0-65536) (可选) UDP记帐

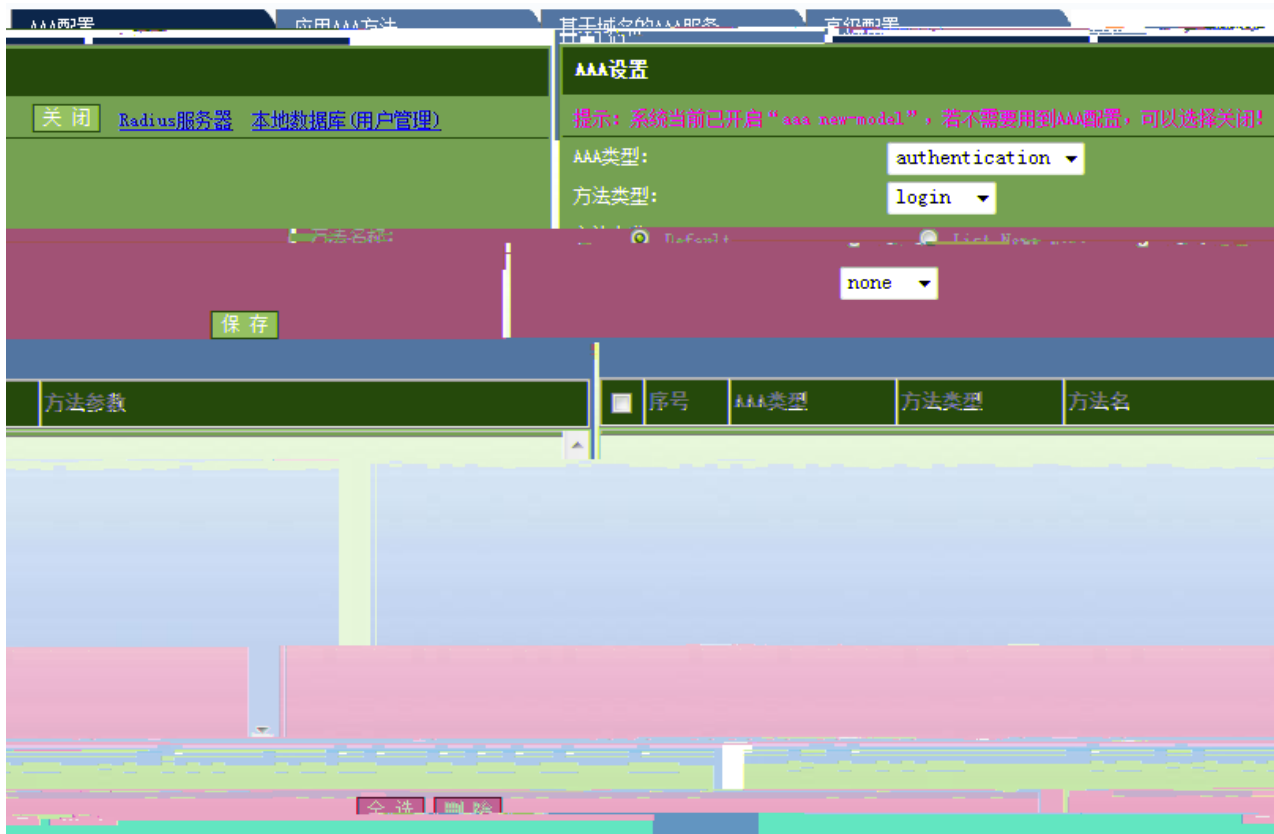
保存

服务器组管理: radius

```
=====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
e

192.168.1.100
Accounting
State:Active



53 AAA

1 AAA

```

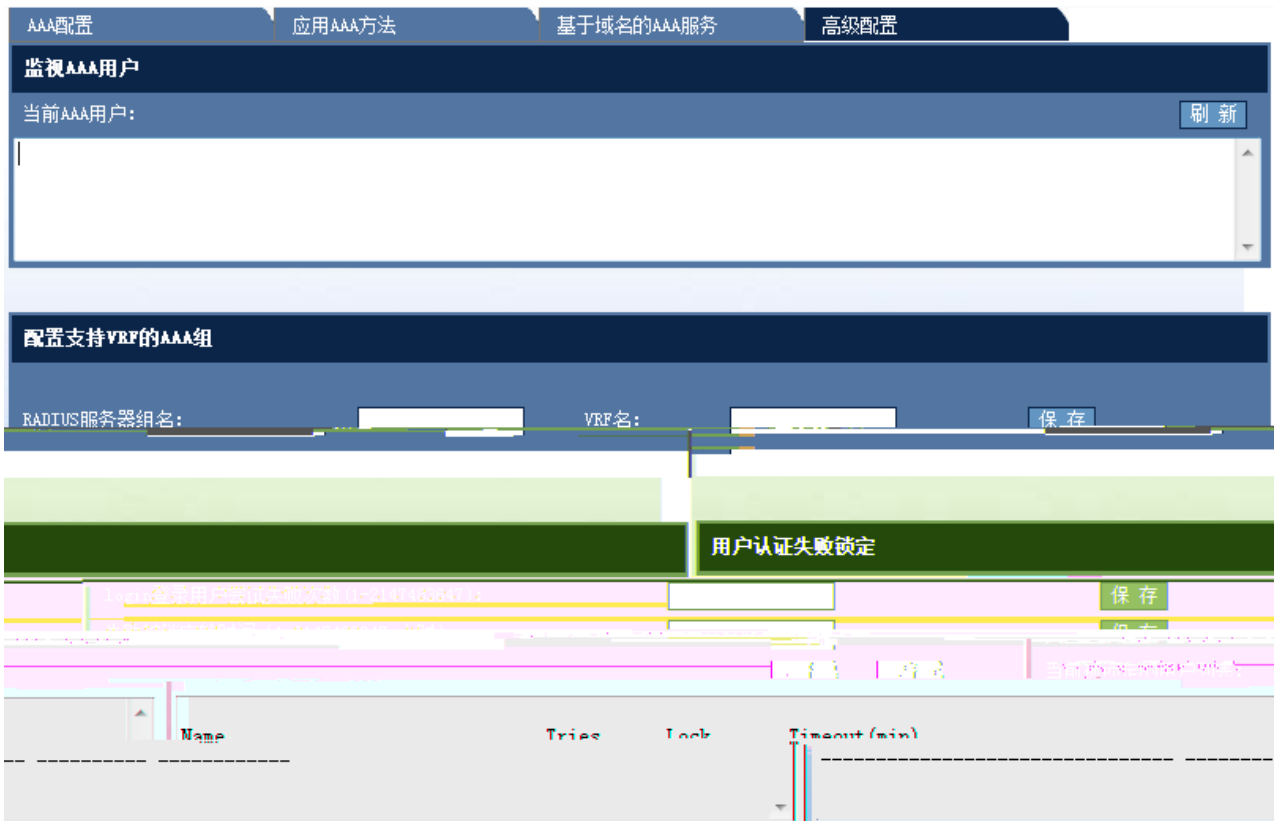
AAA          authentication authorization accounting
AAA          login enable ppp dot1x  exec command network
List Name                                local

```

group

2 AAA





56 AAA

AAA

AAA

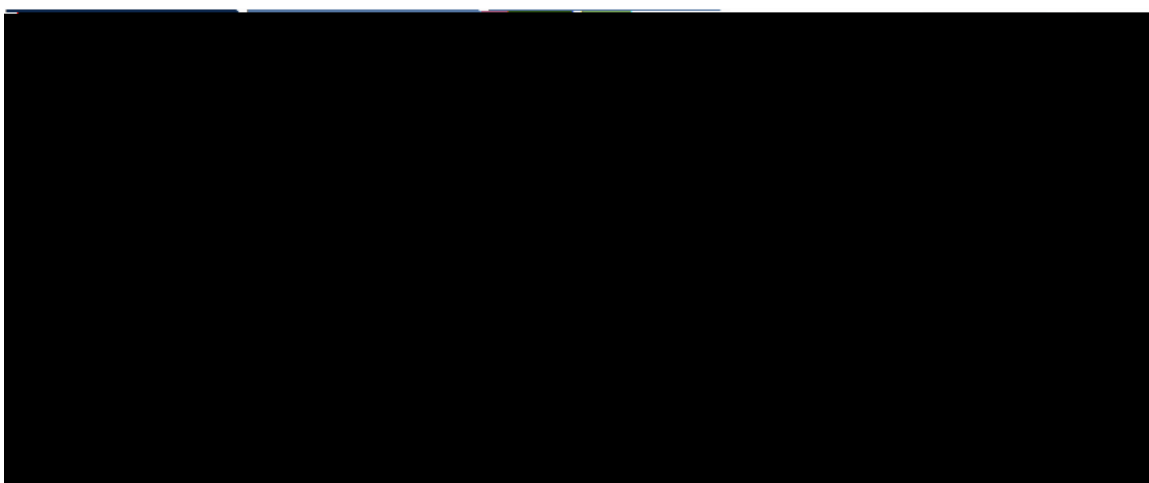
VRF

AAA

2.3.11 Dot1x

" Dot1x "

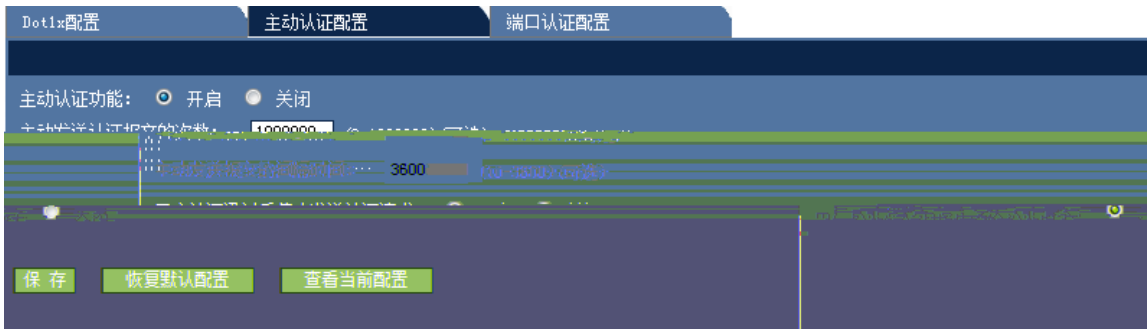
1 Dot1x



57 Dot1x

Dot1x

2



58

3

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

<input type="checkbox"/>	主机MAC地址	端口
<input checked="" type="checkbox"/>	0011.1111.2323	FastEthernet 0/1

60

2

802.1x

MAC

VLAN

2.3.12

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:

■	序号	IP	■	MAC

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	0015.00.70...	1	绑定
4	192.168.23.70	0015.00.70...	1	绑定
5	192.168.23.76	0015.00.70...	1	绑定
6	192.168.23.80	0015.00.70...	1	绑定
7	192.168.23.84	0015.00.70...	1	绑定

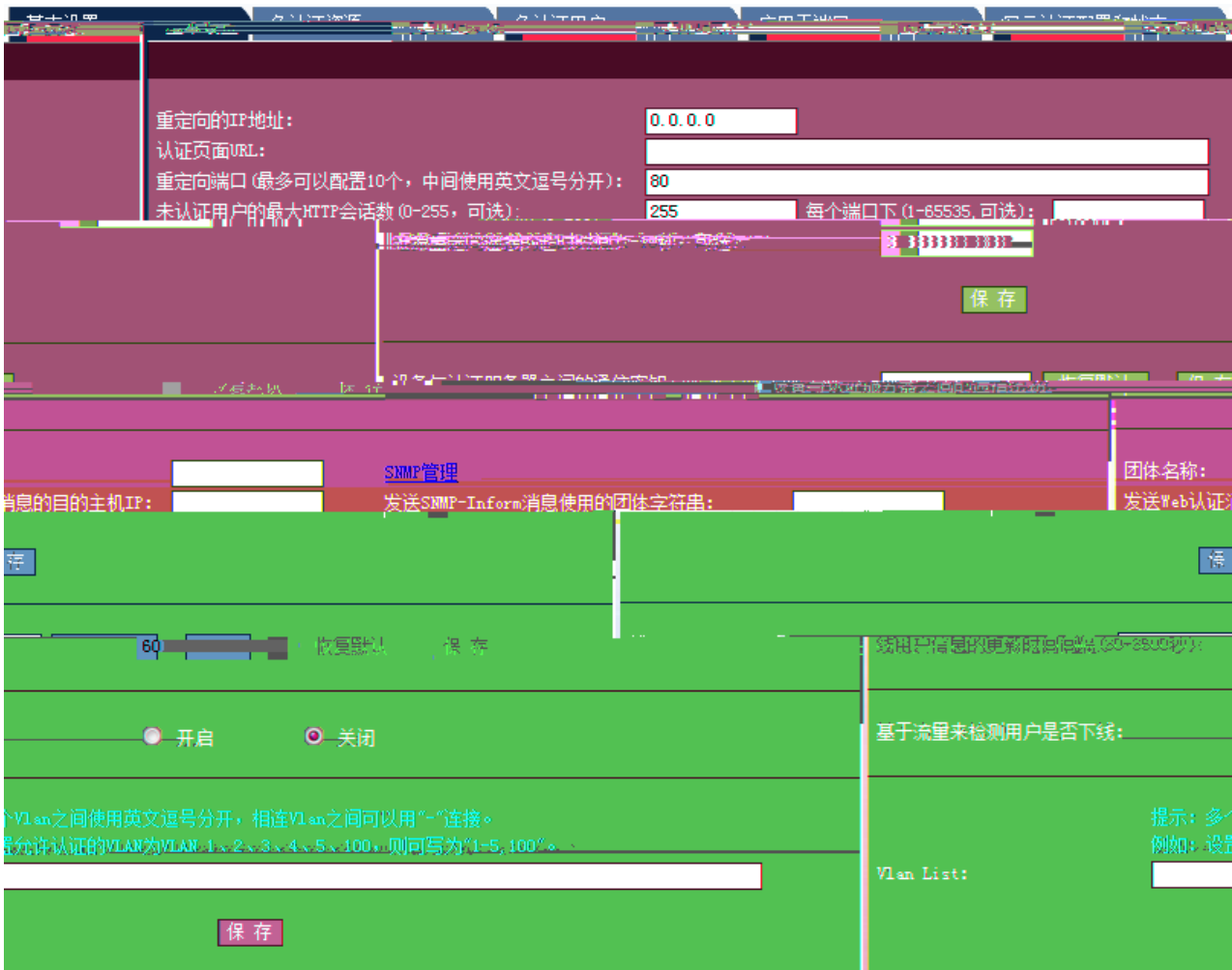
刷新

62 ARP

2.3.13 WEB

" web "

web



63 web

1) web

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

2)



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。

DHCP Snooping 全局配置之使能 DHCP Snooping 全局配置之使能

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
▲	FastEthernet 0/1	使能	10000000



2.4.2



70

DSCP

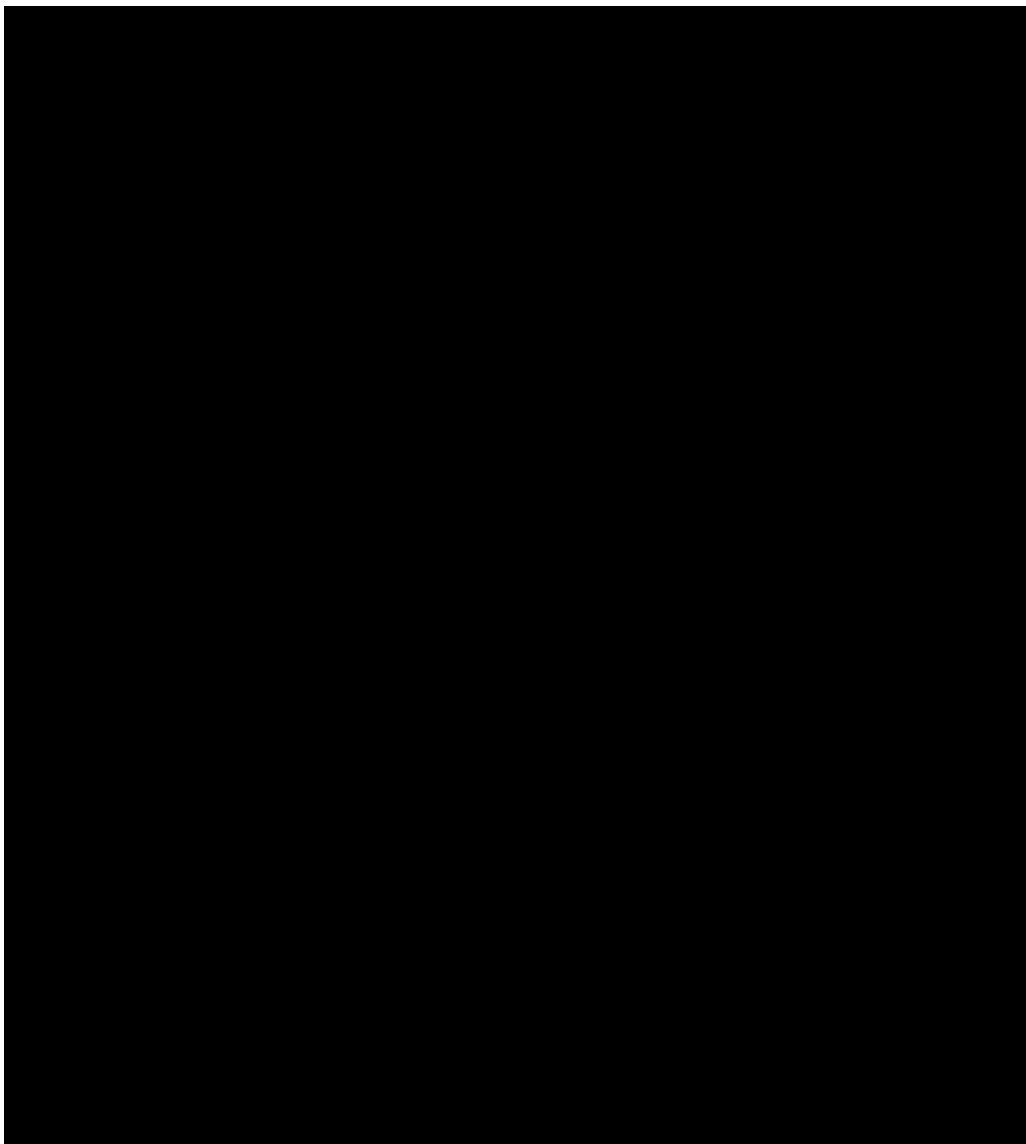
" "

" "

" "

2.4.3

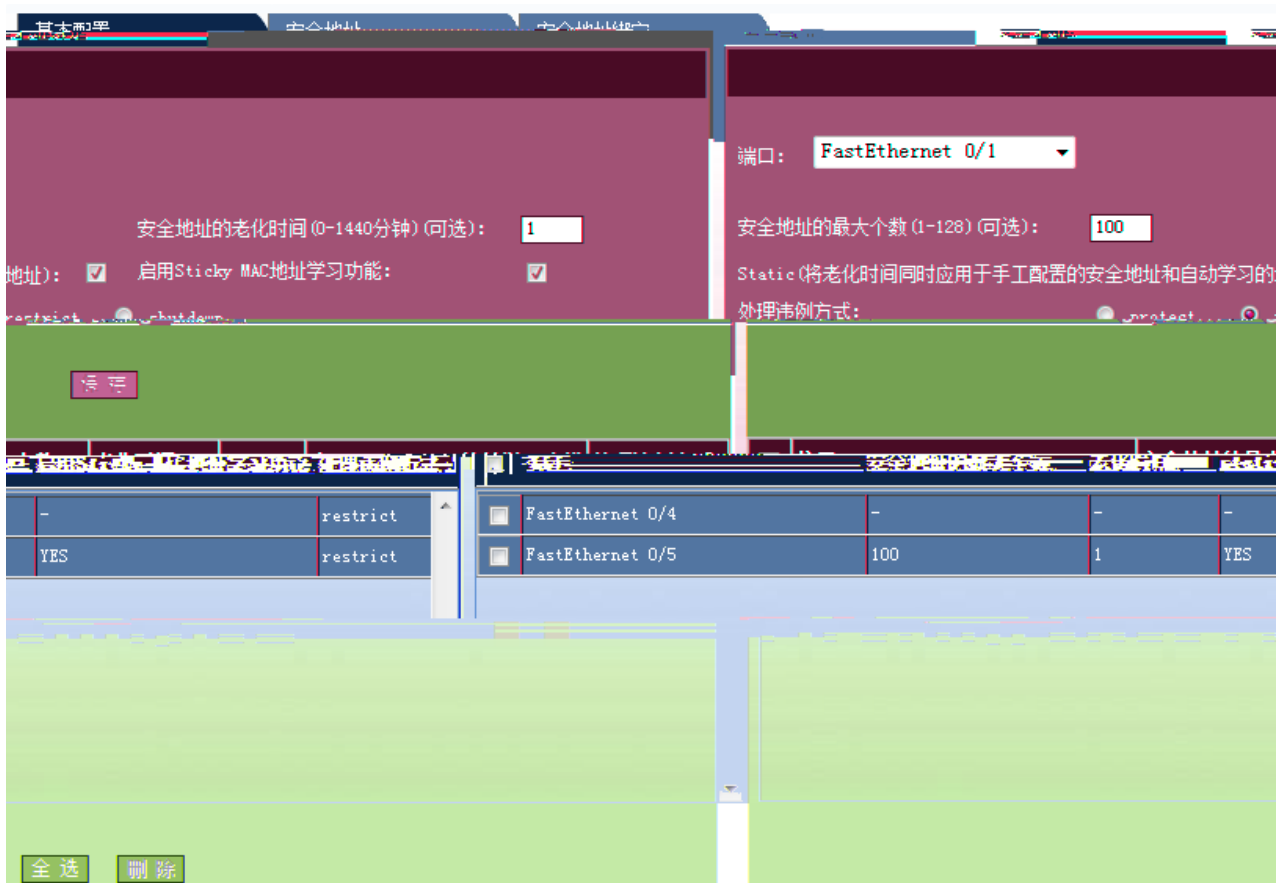
" "





2.4.5

" "



73

1)

Sticky Mac

Static

" "

2)



74

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

76

2.5.2

" " " "

端口状态

端口	类型	名称	状态	速率	模式	速度
down	copper	FastEthernet 0/1	down	1	Unknown	Unknown
down	copper	FastEthernet 0/2	down	2	Unknown	Unknown
up	copper	FastEthernet 0/3	up	1	Full	100
down	copper	FastEthernet 0/4	down	900	Unknown	Unknown
down	copper	FastEthernet 0/5	down	1	Unknown	Unknown
down	copper	FastEthernet 0/6	down	1	Unknown	Unknown
down	copper	FastEthernet 0/7	down	1	Unknown	Unknown
down	copper	FastEthernet 0/8	down	1	Unknown	Unknown
down	copper	FastEthernet 0/9	down	1	Unknown	Unknown
down	copper	FastEthernet 0/10	down	1	Unknown	Unknown

刷新

78

2.5.4

" "

端口运行状态

端口	带宽占用
FastEthernet 0/1	low
FastEthernet 0/2	low
FastEthernet 0/3	low
FastEthernet 0/4	low
FastEthernet 0/5	low
FastEthernet 0/6	low
FastEthernet 0/7	low
FastEthernet 0/8	low
FastEthernet 0/9	low
FastEthernet 0/10	low

刷新

79

2.5.5

端口统计信息

注意：选择 All Ports 时，将增加所有端口的统计信息。

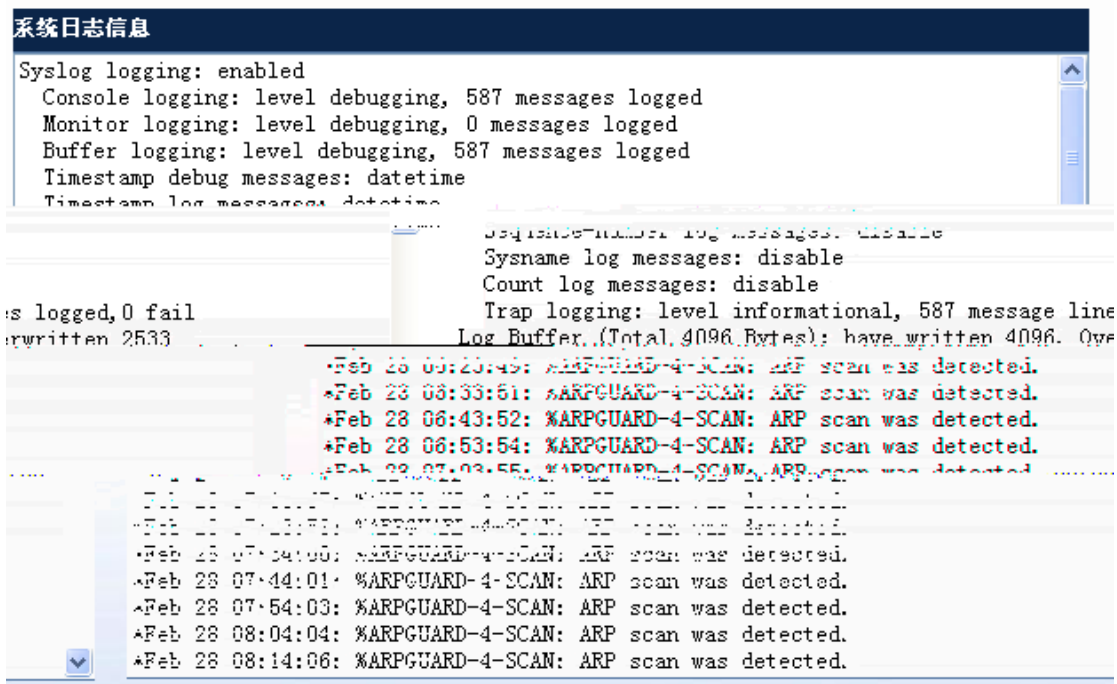
端口：

输入/输出帧统计

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	0	0	0	Gi0/2	0	0	0	0
2717	0	0	0	Gi0/3	6	5	6264	3004
0	0	0	0	Gi0/4	0	0	0	0
175	0	0	0	Gi0/5	34	23	11	0
0	0	0	0	Gi0/6	0	0	0	0
2298818	0	0	0	Gi0/7	882792	404167	69848	408777
0	0	0	0	Gi0/8	0	0	0	0
842417	0	0	0	Gi0/9	437082	435647	37	1398
0	0	0	0	Gi0/10	0	0	0	0
2367132	0	0	0	Gi0/11	856226	850552	149	5525
0	0	0	0	Gi0/12	0	0	0	0
0	0	0	0	Gi0/13	0	0	0	0
0	0	0	0	Gi0/14	0	0	0	0
8386	0	0	0	Gi0/15	5557815	1423231	935630	3198954
0	0	0	0	Gi0/16	0	0	0	0

80

2.5.6



81

2.6

2.6.1 Ping

" Ping"

Ping



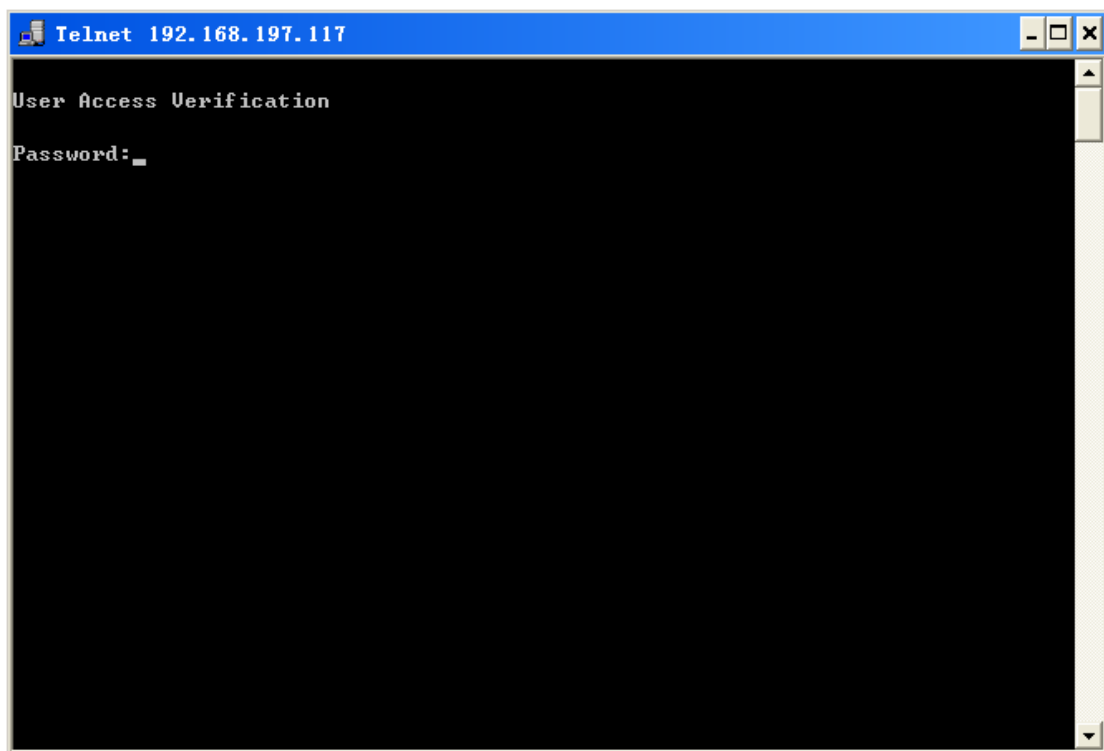
82 Ping

IP " " IP Ping

2.6.2 Telnet

" Telnet"

Telnet



83 Telnet

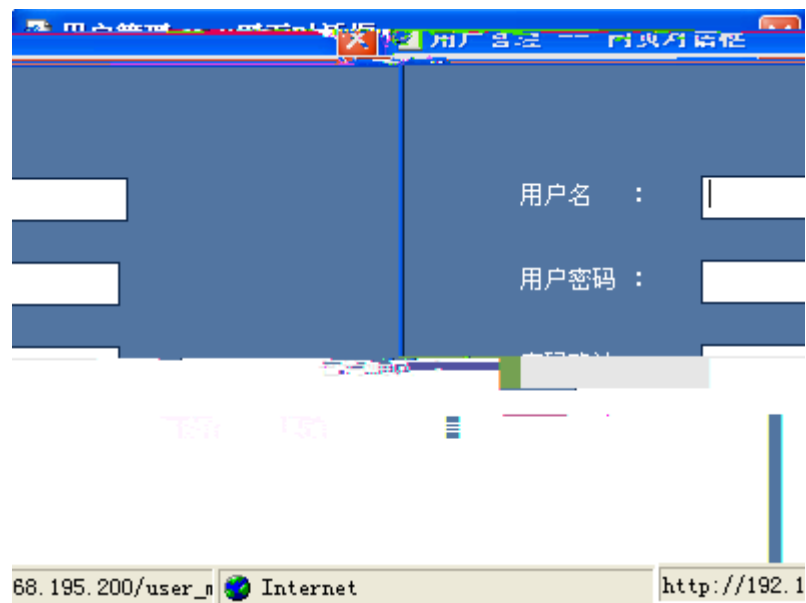
PC " Telnet" Telnet PC Telnet

2.6.3

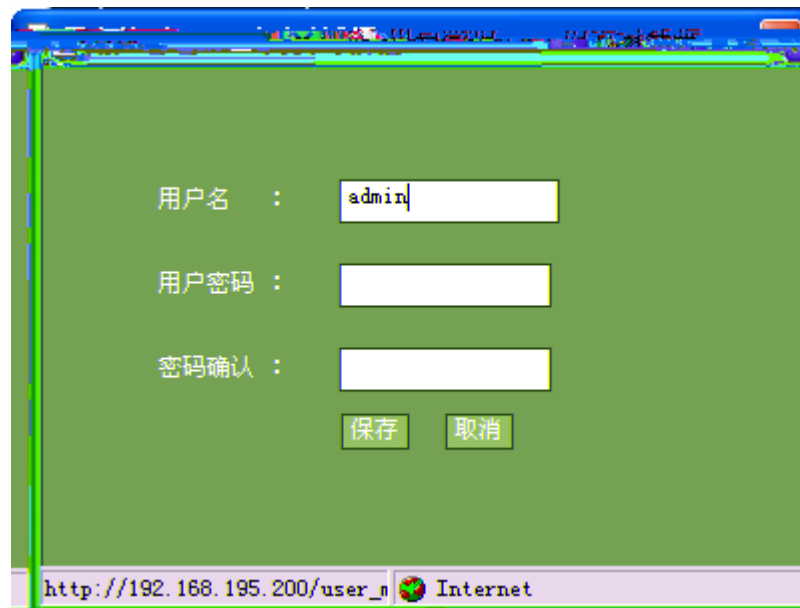
" "



84



85



86

" "

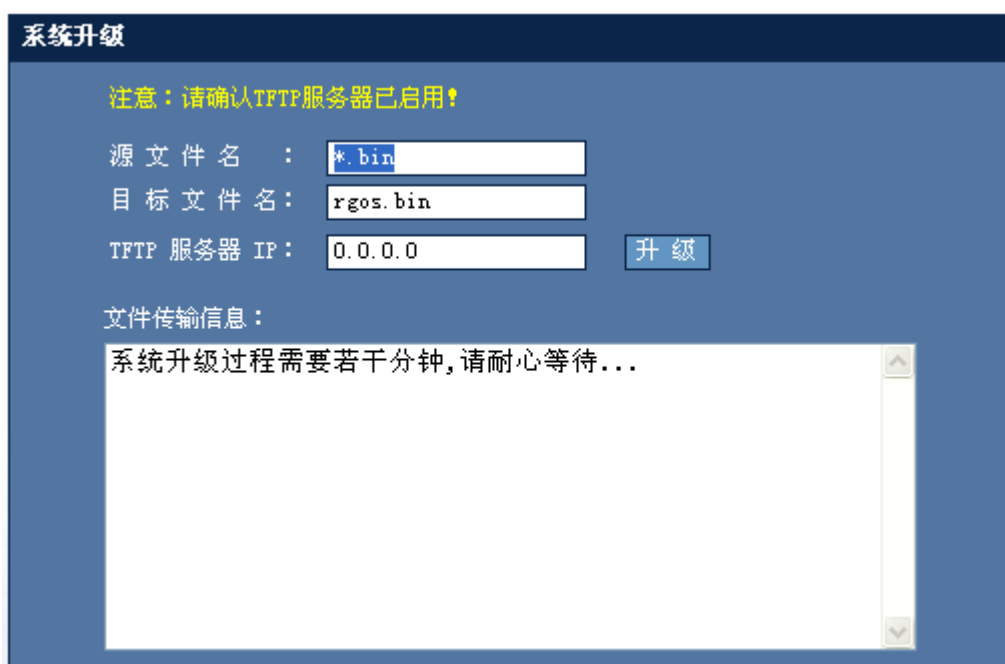
" "

8080 IP 192.168.1.1

_____ :8080 " "

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

b. WEB

c. WEB Local

d. 15

e. IP

-
- 2 Enable
 - a. config
 - b. WEB
 - c. WEB Enable
 - d. Enable
 - e. IP

2.8.5

- 1 Local

```
//WEB
//WEB 15
//WEB local
!
// WEB
```

160BT/F12 10.5 Tf1 0 0 1 100.52 247.16 Tm[1

// IP

2 Enable

0terface VLAN 1

//WEB Enable

