



WEB

RG-AS3GT

RGOS 10.4(3b16)p5

V1.0

©2015



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

1)

[] []

{x|y|...}

[x|y|...]

//

2)

3)

1 WEB

1.1 WEB

WEB

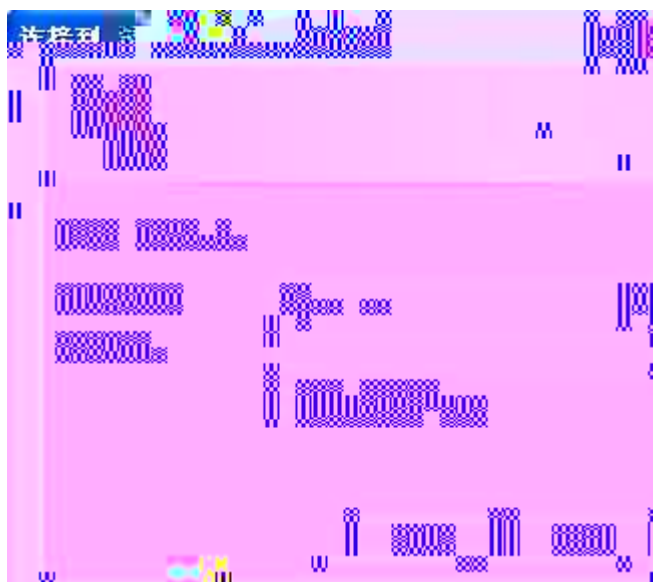
IE

1-1

交换机 WEB 管理平台



1-2



WEB

1-3 WEB



1.5

1.5.1



ip " "

1-5 IP



IP " "

1.5.2 VLAN

" VLAN "

VLAN

1-6 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上独立的广播域，从而实现不同用户或部门之间的隔离和通信。

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

新建 全选 删除 修改

VLAN

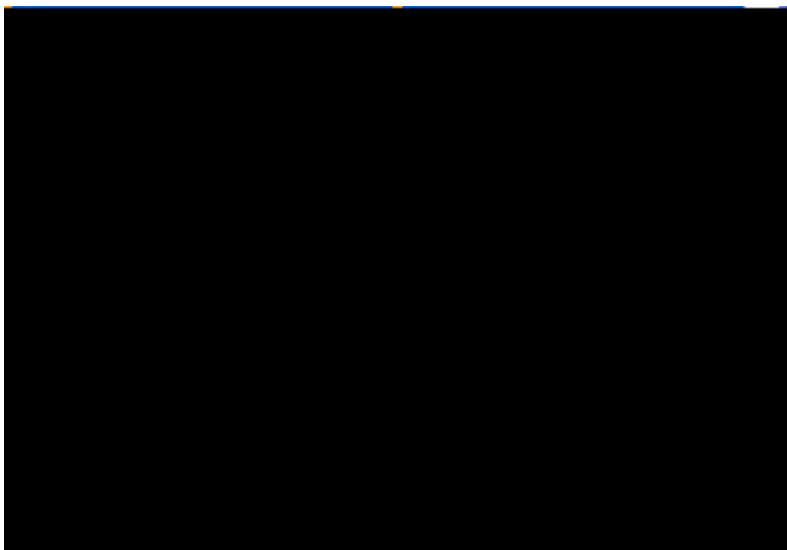
VLAN

VLAN

VLAN

" "

1-7 VLAN



VLAN ID VLAN

" "

VLAN

VLAN

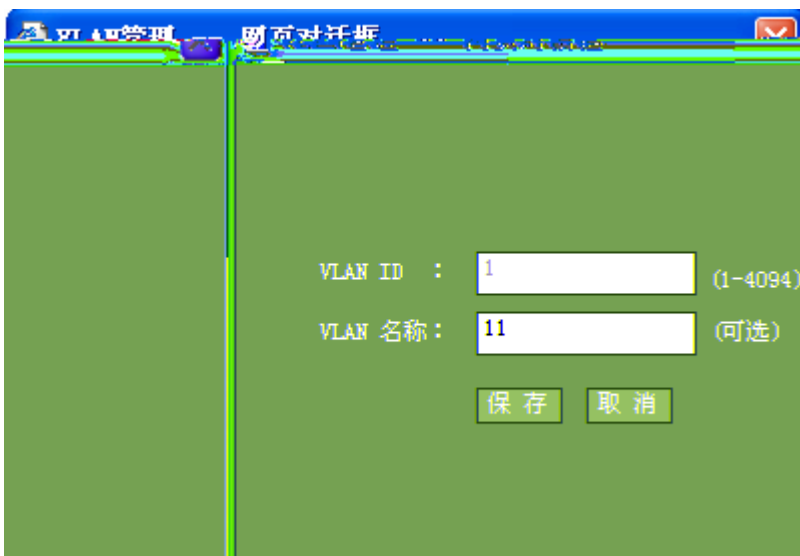
VLAN

" "

VLAN

" "

1-8 VLAN



VLAN

" "

VLAN

VLAN

1-9 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

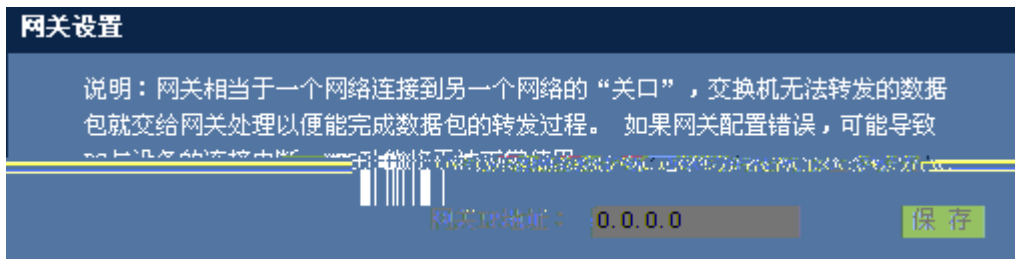
保存

VLAN ID " "

1.5.3

" "

1-10



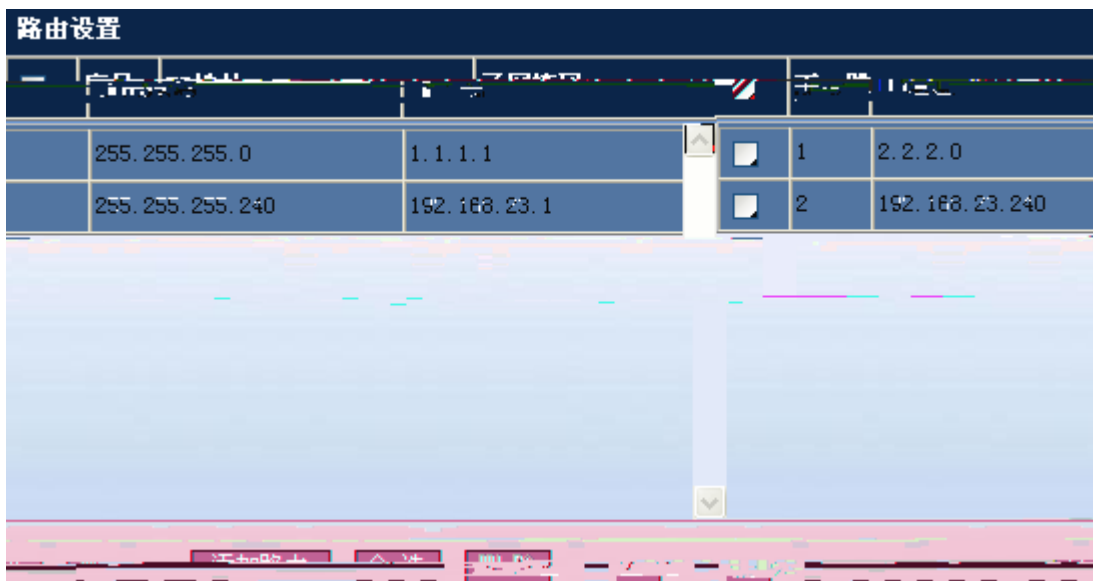
IP " "

IP

1.5.4

" "

1-11



" "

1-12



1.5.6

1-14



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。

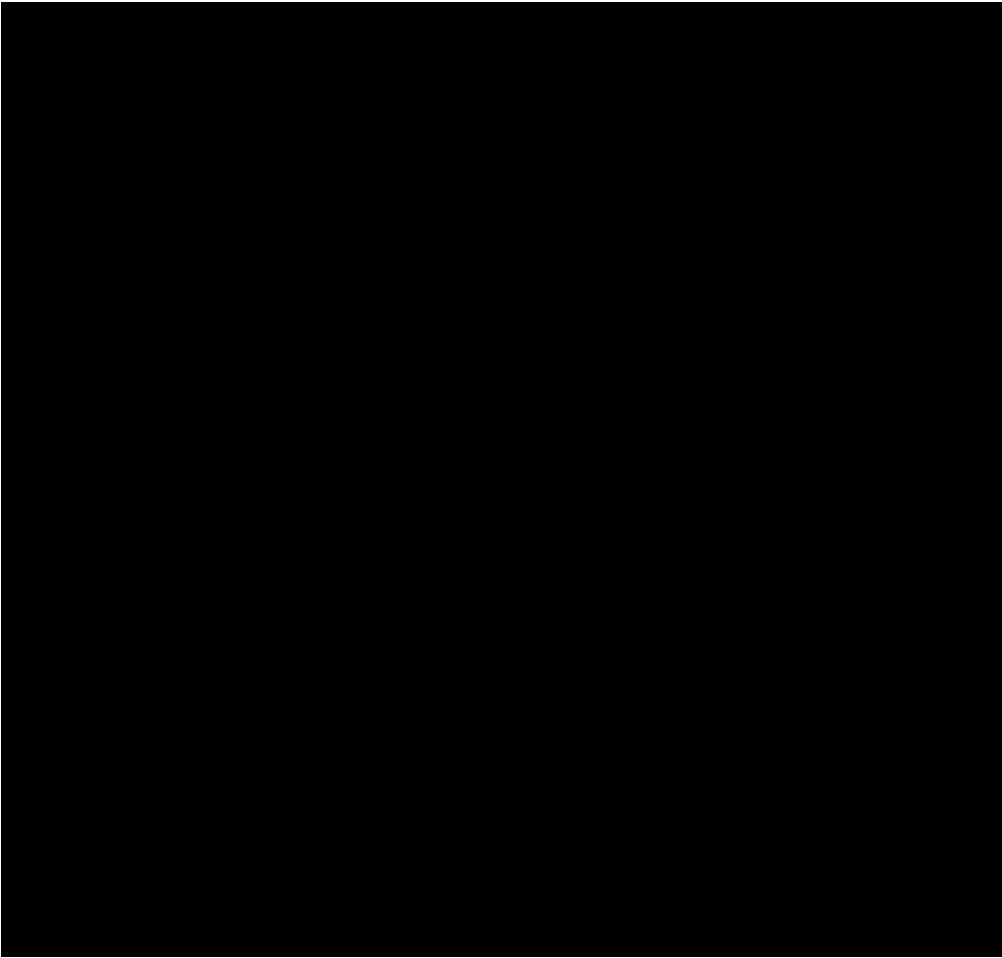
端口	输出速率限制 (64-1000000 KBit/s)	瞬时速率限制 (4-16380 K)
GigabitEthernet 0/1	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/2	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/3	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/4	<input type="text"/>	<input type="text"/>
GigabitEthernet 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
保存

1.5.7



1-17



" "

" "

1.5.8

" "

1-18

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	10	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	Up	Full	100	Off	-
Gi0/12	Down	Auto	Auto	Off	-

" "

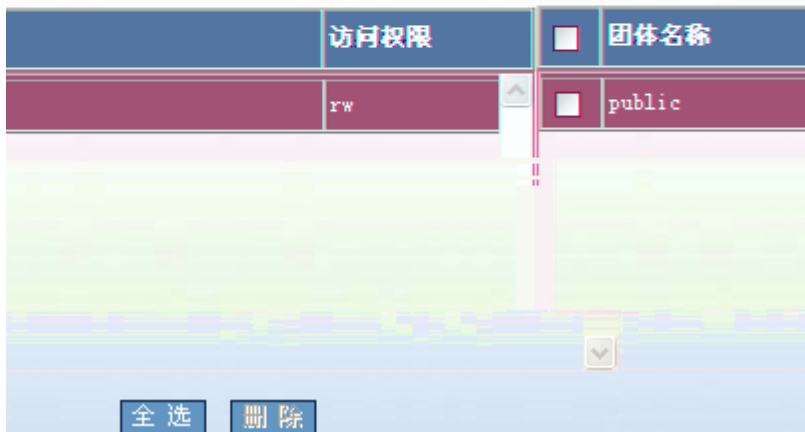
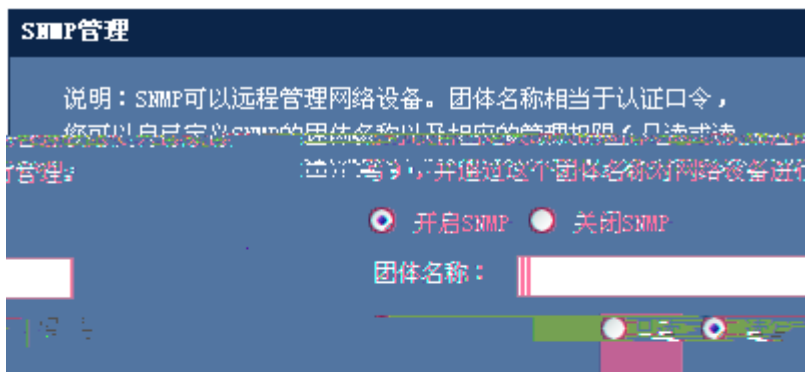
1.5.9 DHCP

" DHCP "

DHCP

1-19 DHCP





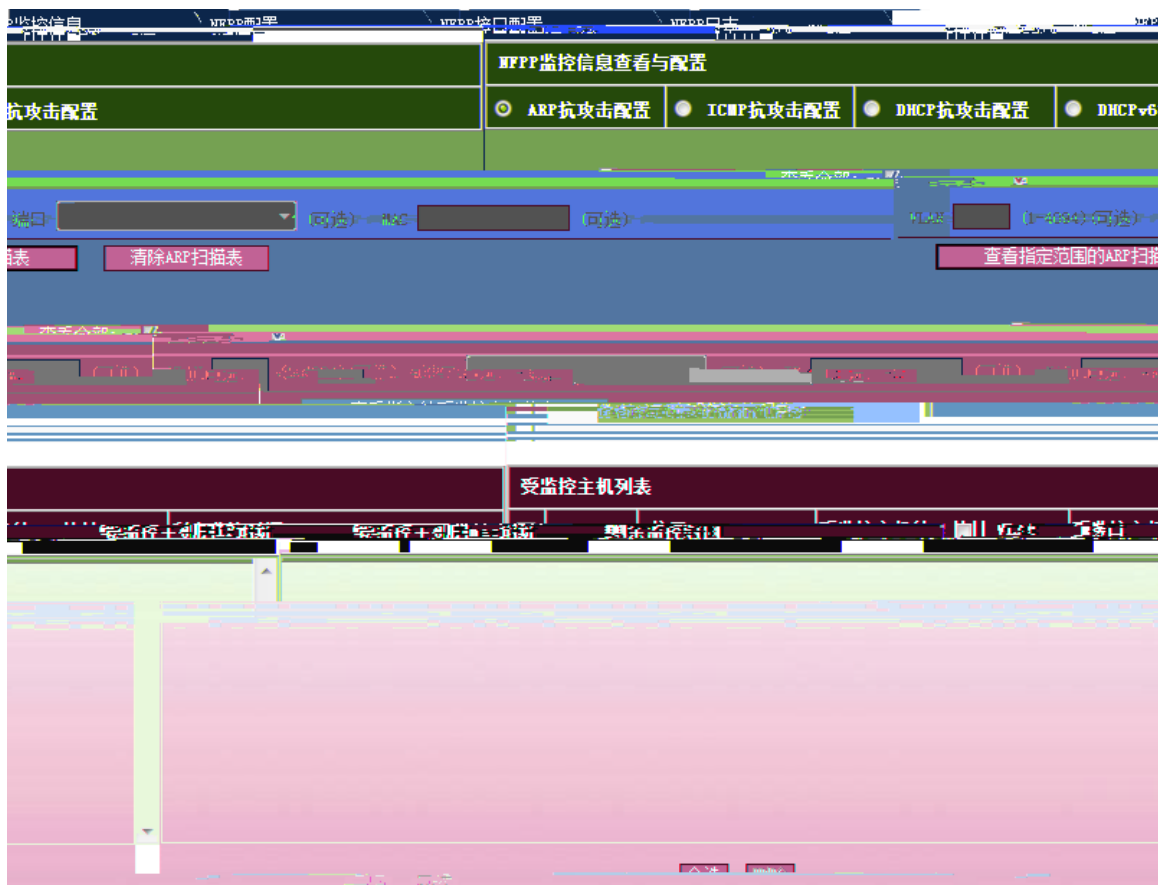
SNMP " SNMP" " SNMP" " "

1.5.13 NFPP

" NFPP "

NFPP

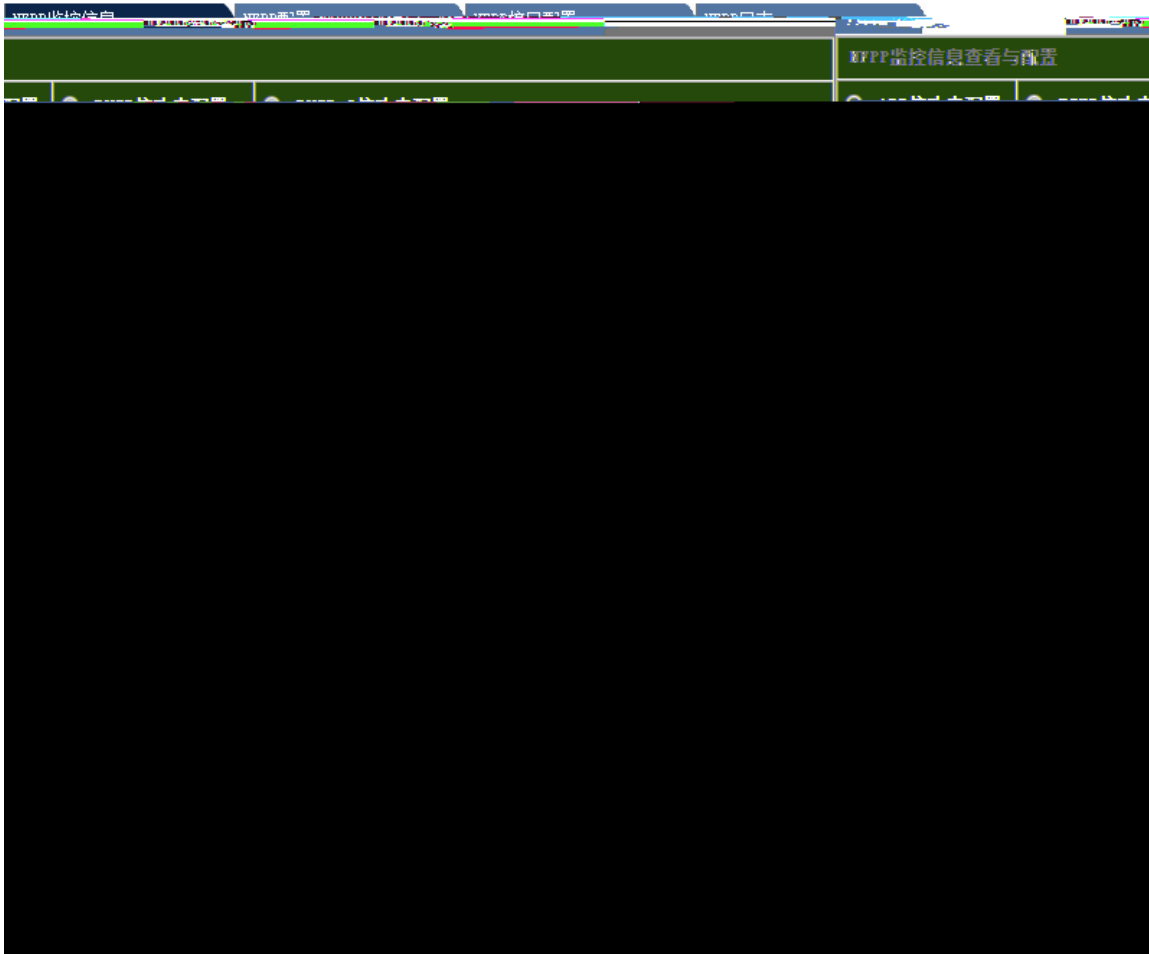
1-23 NFPP



NFPP

1) ARP

1-24 NFPP —ARP



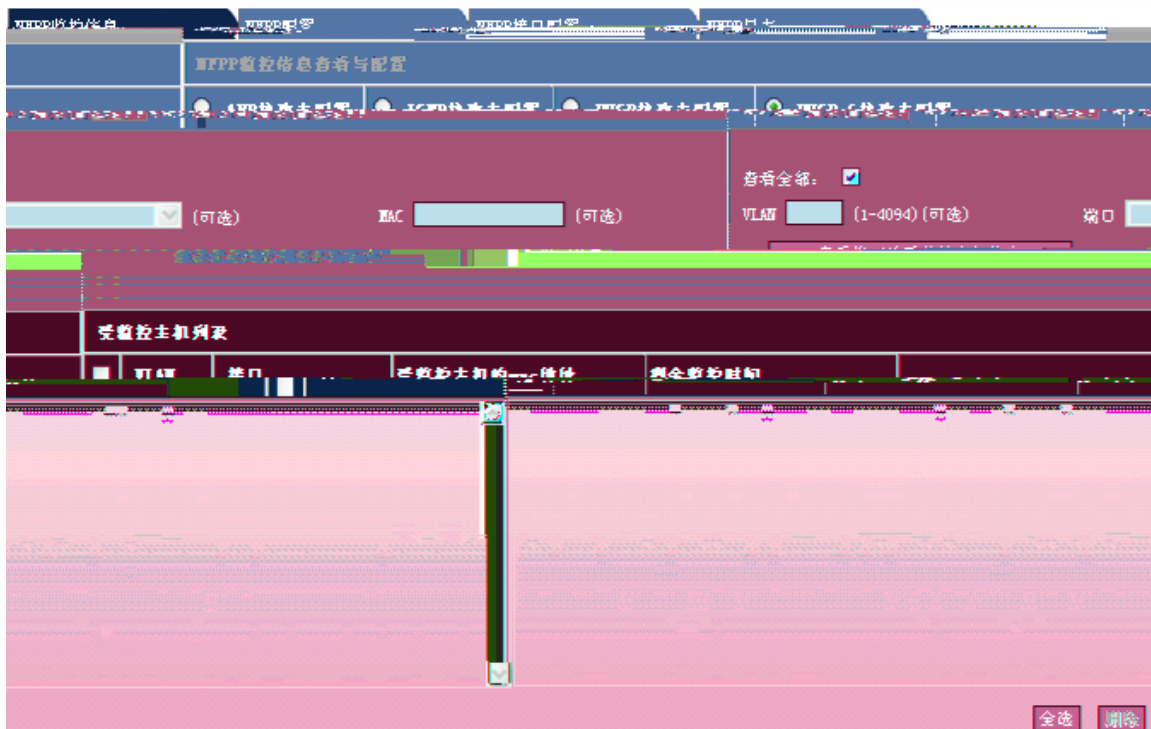
ARP



DHCP

4) DHCPv6

1-27 NFPP —DHCPv6



DHCPv6

NFPP

1-28 NFPP

NFPP监控信息 NFPP配置 NFPP接口配置 NFPP日志

Manage报文比例	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
-	-	-	-	-	-

修改 恢复默认

DHCP	DHCPv6	ND	协议类型:	ARP	ICMP
Enable	Enable	Enable	Enable	Enable	状态:
0	0	0	0	-	隔离时间:
600s	-	监控时间:	600s	600s	600s
1000	-	最大监控主机数:	1000	1000	1000
-/5/150	15/15/15	基于IP识别限速/基于mac识别限速/全局端口限速:	4/4/100	100/-/200	-/5/150
-/10/300	30/30/30	攻击阈值 (基于ip识别/基于mac识别/全局端口):	8/8/200	100/-/200	-/10/300
-	-	扫描阈值:	15	-	-
恢复默认	恢复默认	恢复默认值:	恢复默认	恢复默认	恢复默认

修改 恢复默认

1) CPU

1-29 CPU

网页对话框

Protocol报文带宽: (1-8192) (可选)

Route报文带宽: (1-8192) (可选)

Manage报文带宽: (1-8192) (可选)

Protocol报文比例: (1-98) (可选)

Route报文比例: (1-98) (可选)

Manage报文比例: (1-98) (可选)

保存 取消

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



ICMP

NFPF

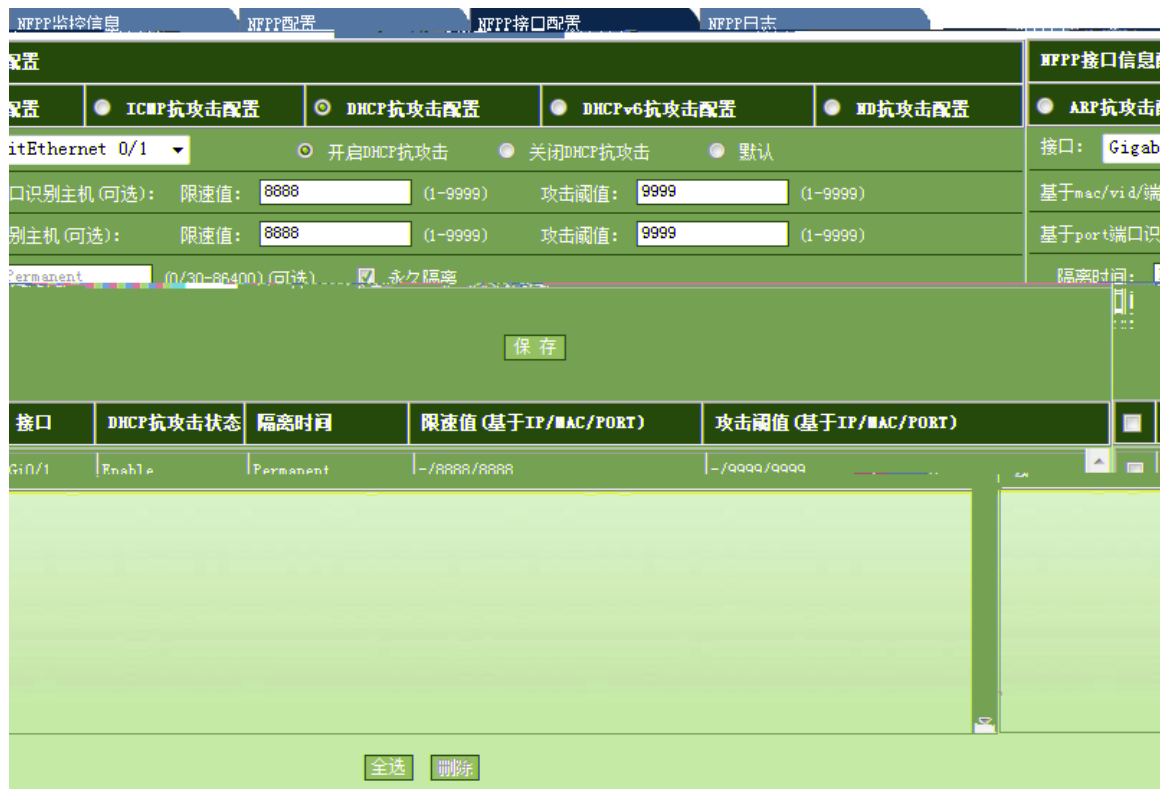
" "

3) DHCP

1-33 NFPF

—NFPF

DHCP



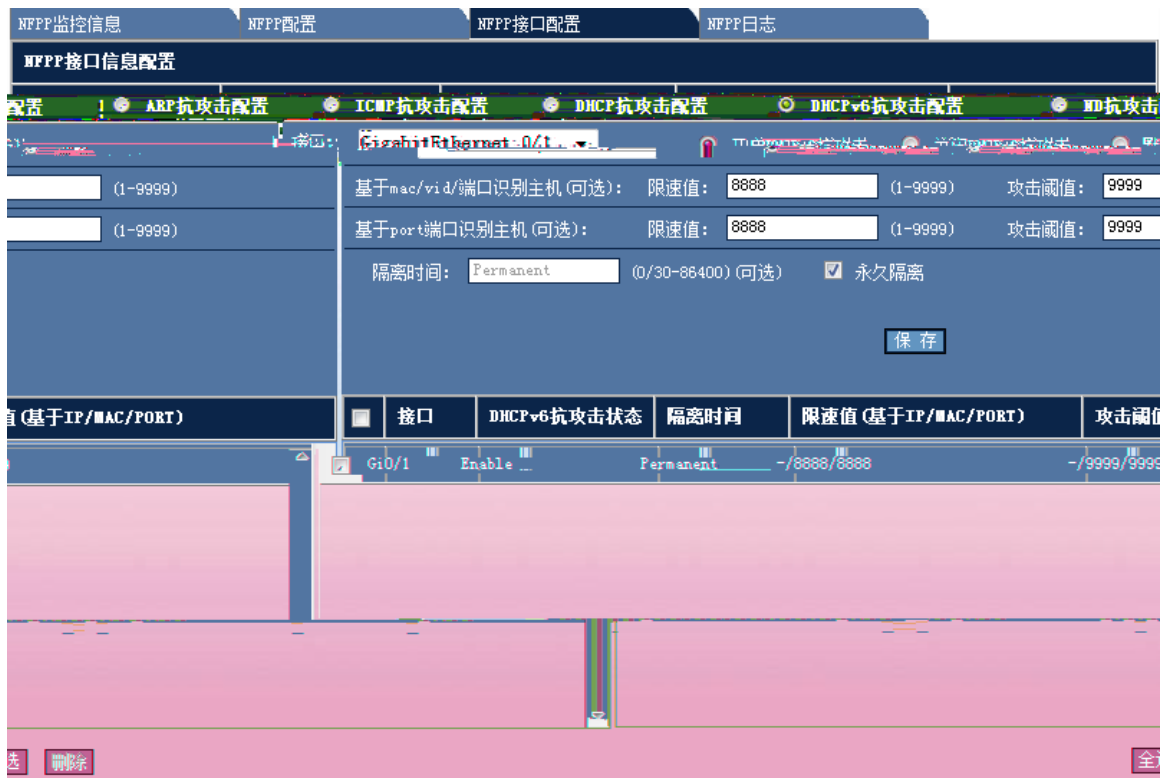
DHCP

NFPP

" "

4) DHCPv6

1-



DHCPv6

NFPF

" "

5) ND

1-35 NFPF

—NFPF

ND



ND

NFPF

" "

NFPF

1-36 NFPF

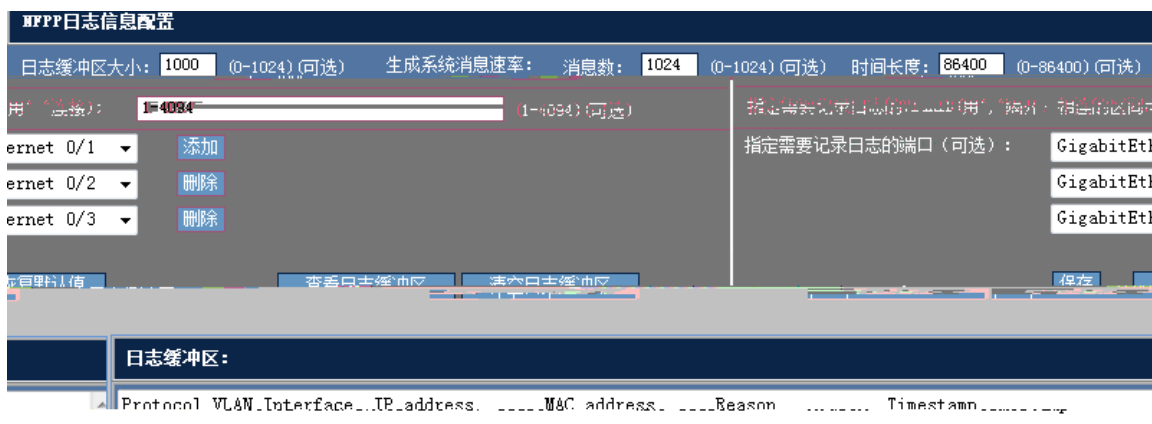


NFPP

" "

" "

1-37



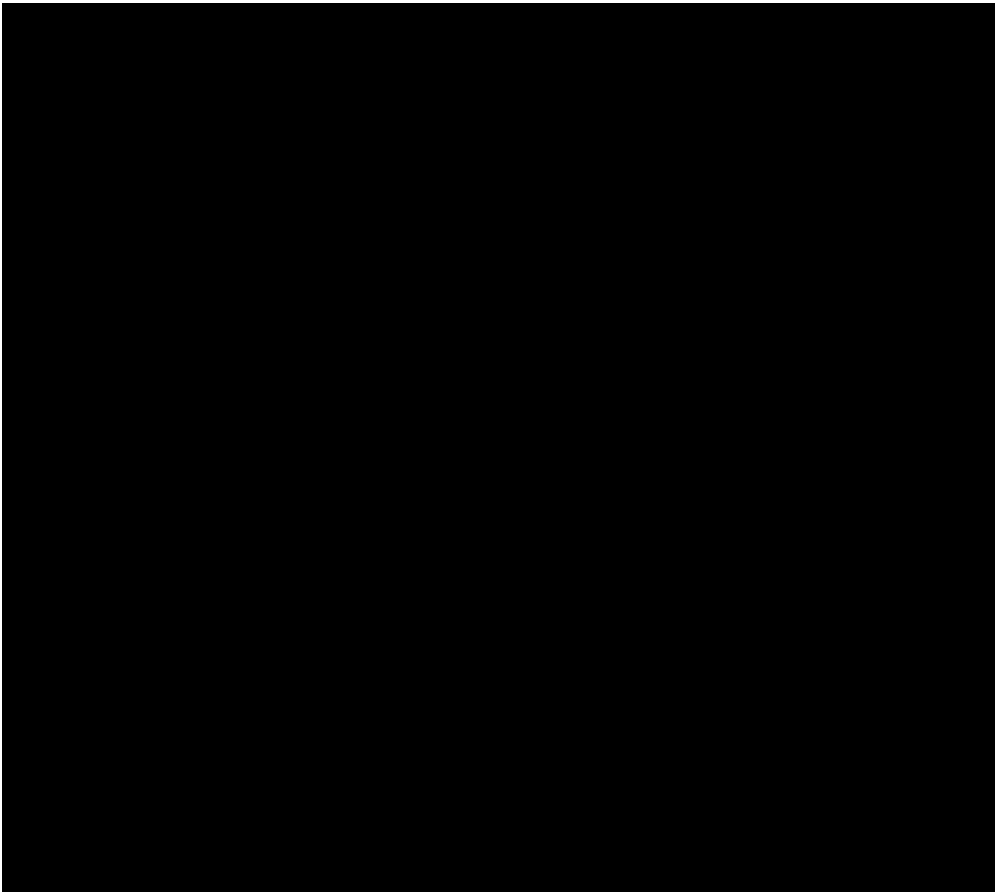
1.6

1.6.1 ARP

" ARP "

ARP

1-38 ARP



" "

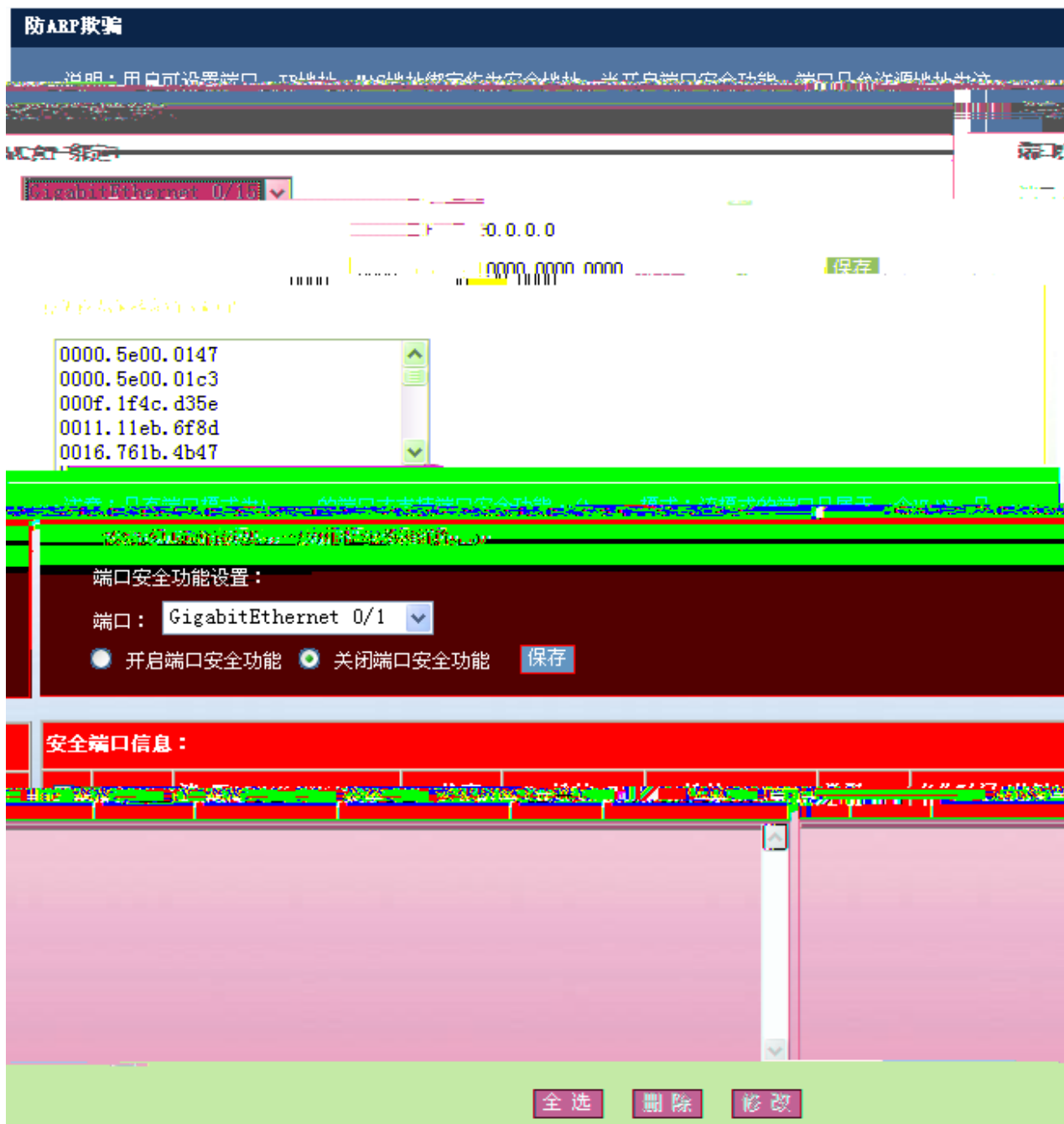
" "

1.6.2 ARP

" ARP "

ARP

1-39 ARP



/MAC/IP

/MAC/IP

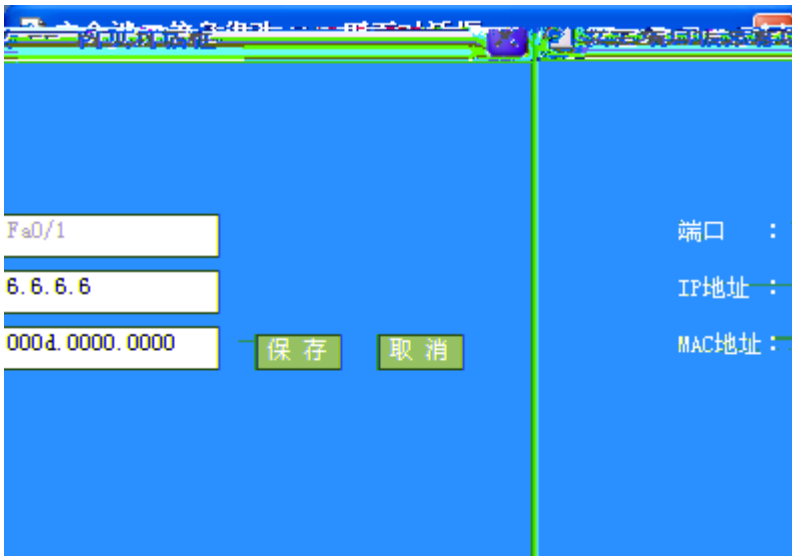
IP MAC " "

MAC

GigabitEthernet 0/15

MAC

1-40



1.6.3 ARP

" ARP "

ARP

1-41 ARP



" ARP "

" ARP "

1.6.4 ACL

" ACL "

ACL

1-42 ACL

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访问列表 配置标准IP访问列表

规则：禁止

列表 ID(名称)：

协议：TCP

源IP地址：
 任意源IP地址：
 指定IP地址范围：0.0.0.0 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：0.0.0.0 通配符掩码： (可选)

目的端口：
 (1-65535) (可选)

保存

ID

TCP UDP IP ICMP

IP

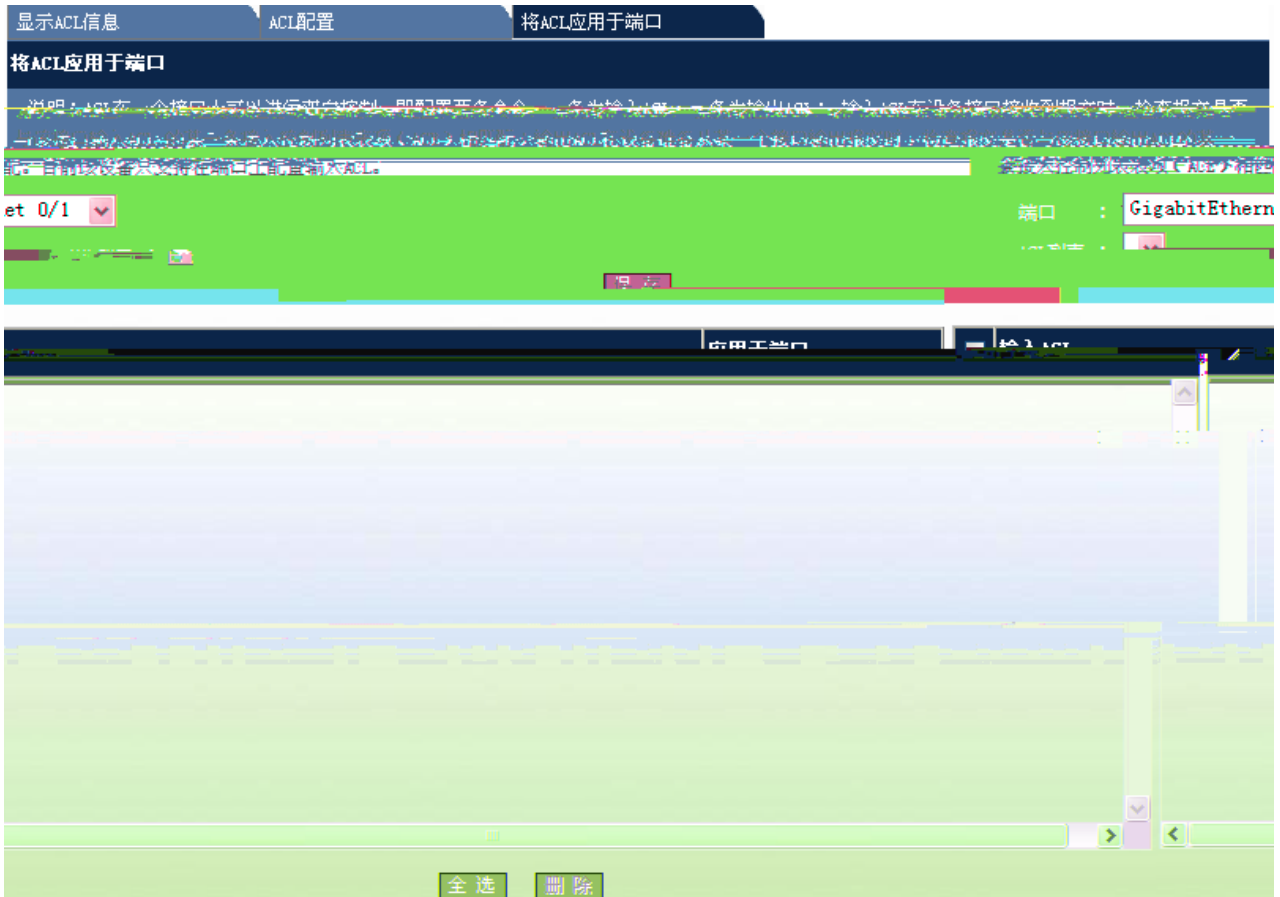
IP

IP

IP

IP

IP



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

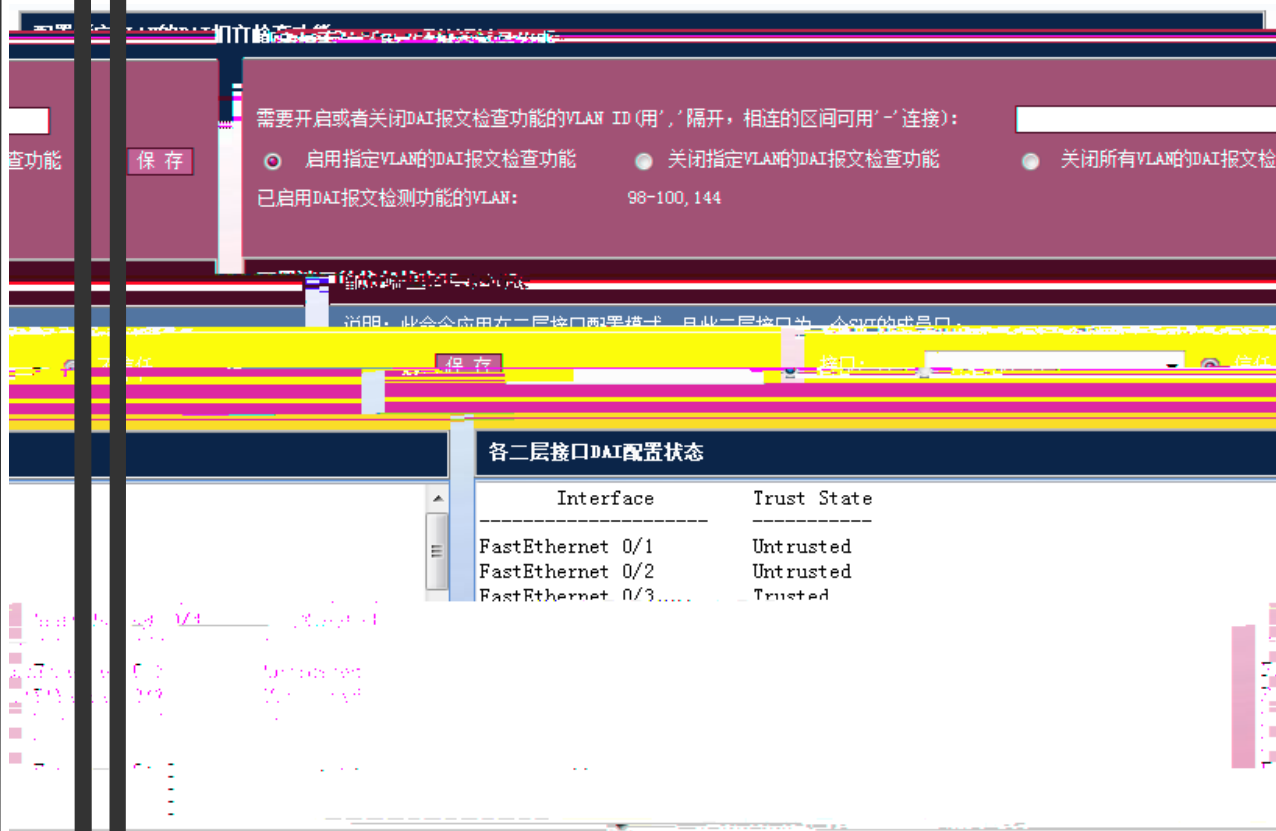
1-46 IP Source Guard



IP Source Guard

IP+MAC " IP+MAC ()"

IP



DAI

VLAN 100 DAI

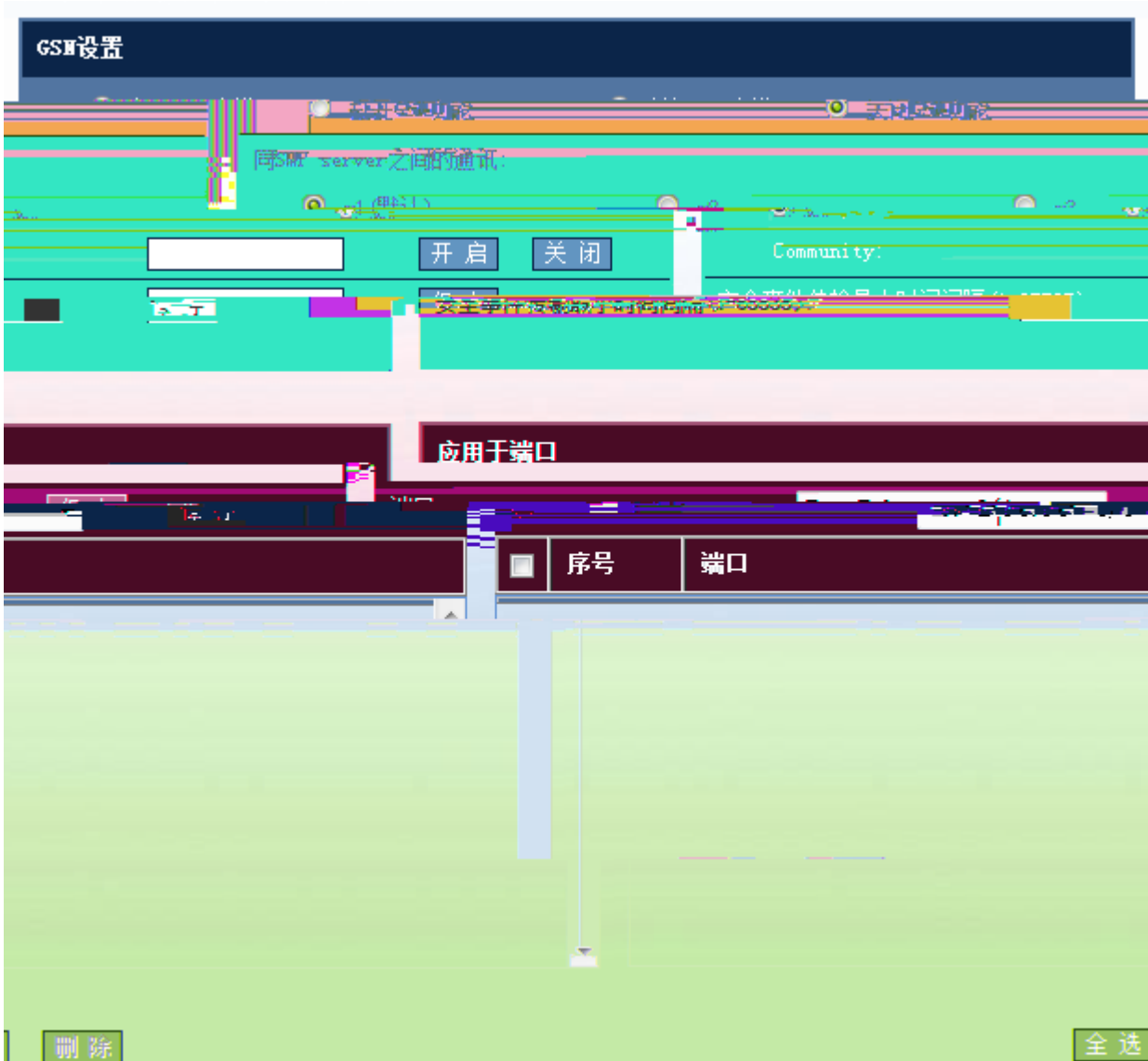
vlan-id 100 ARP

1.6.7 GSN

" GSN"

GSN

1-49 GSN



GSN

GSN

GSN

GSN

GSN

SMP server

SMP server

v1

v2 v3

Community User

" " "

" &

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
tunntel-bpdu	180	6
ipv4-icap-local	1600	6
lldp	180	5
lldp_cdp	180	5

1-53

管理板/单机/堆叠系统的接收报文的统计信息			
Type	Pps	Total	Drop
tp-guard	0	0	0
arp	8	325751	0
dhcp	0	0	0
ospf	0	0	0
igmp	0	0	0
l2mp	0	0	0
l2mp_ospf	0	0	0
ospf	0	0	0
dhcp-ipv4	0	0	0
dhcp-ipv6	0	0	0
l2mp	0	0	0

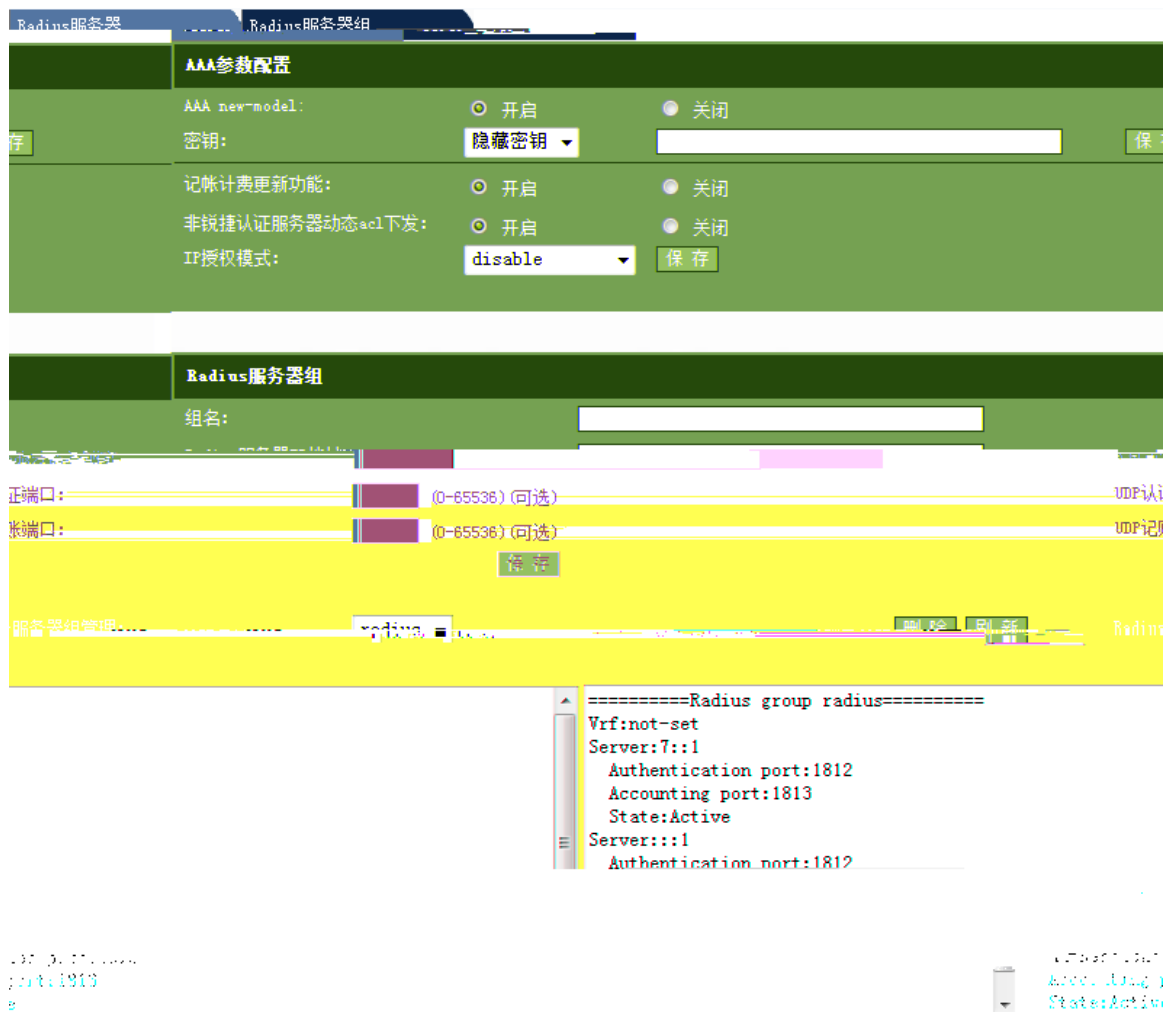
" "

1.6.9 RADIUS

" RADIUS "

RADIUS

1-54 RADIUS



RADIUS IP

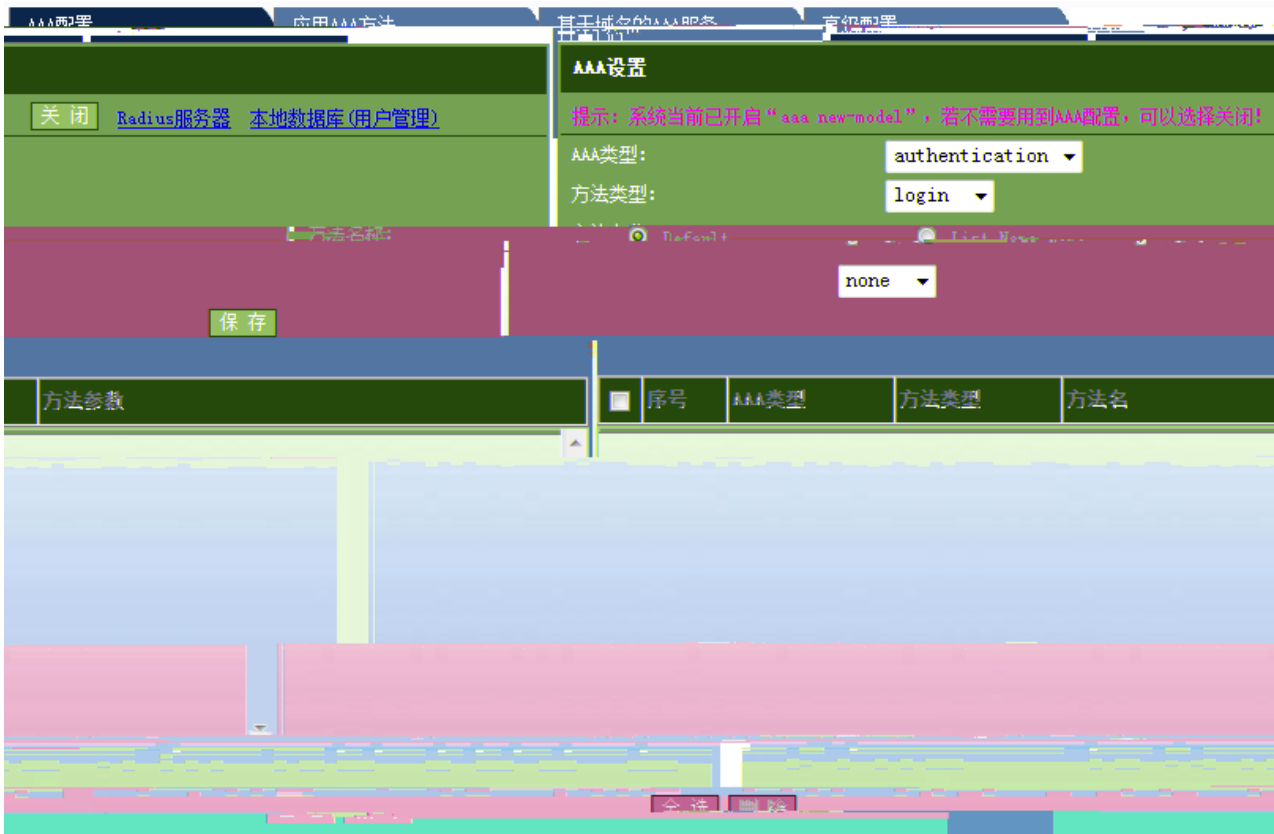
Radius

1.6.10 AAA

" AAA "

AAA

1-56 AAA



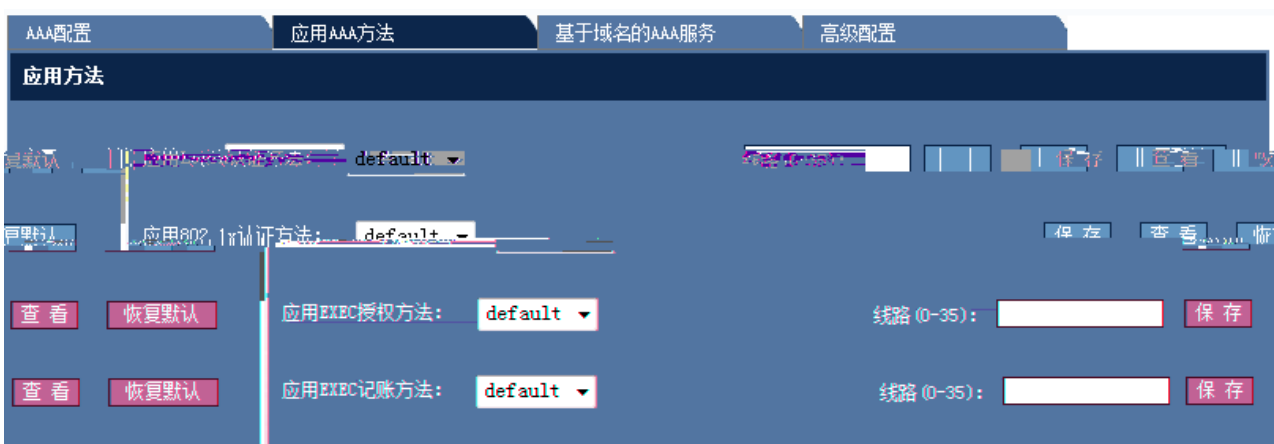
AAA

```

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

AAA

1-57 AAA



AAA

AAA

AAA

1-58

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

Domain Name: Domain Name

域名: Default

Domain认证方法: default

PPP认证方法: default

授权方法 (network): default

记账方法 (network): default

域状态: 由白名单不携带域名信息

Access Limit (1-1024):

AAA Domain管理:

```

=====Domain default=====
State: Block
Username format: With-domain
Access limit: 2
802.1X Access statistic: 0
Selected method list:

```

AAA

Dot1x

PPP

(network)

(network)

Access Limit

AAA Dom



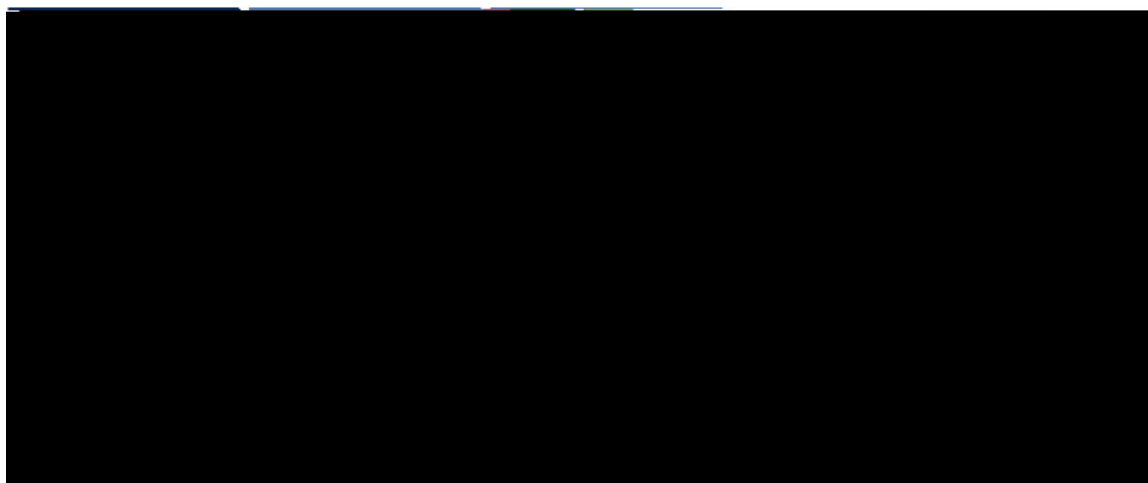
AAA AAA VRF AAA

1.6.11 Dot1x

" Dot1x "

Dot1x

1-60 Dot1x

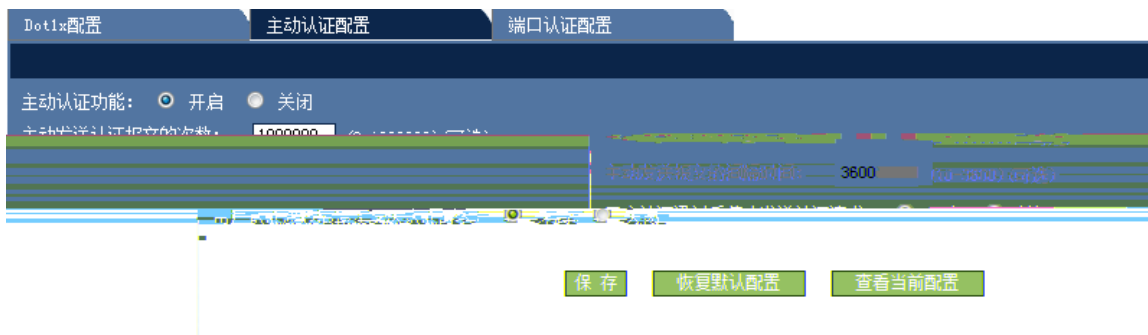


Dot1x

Dot1x

" " " "

1-61



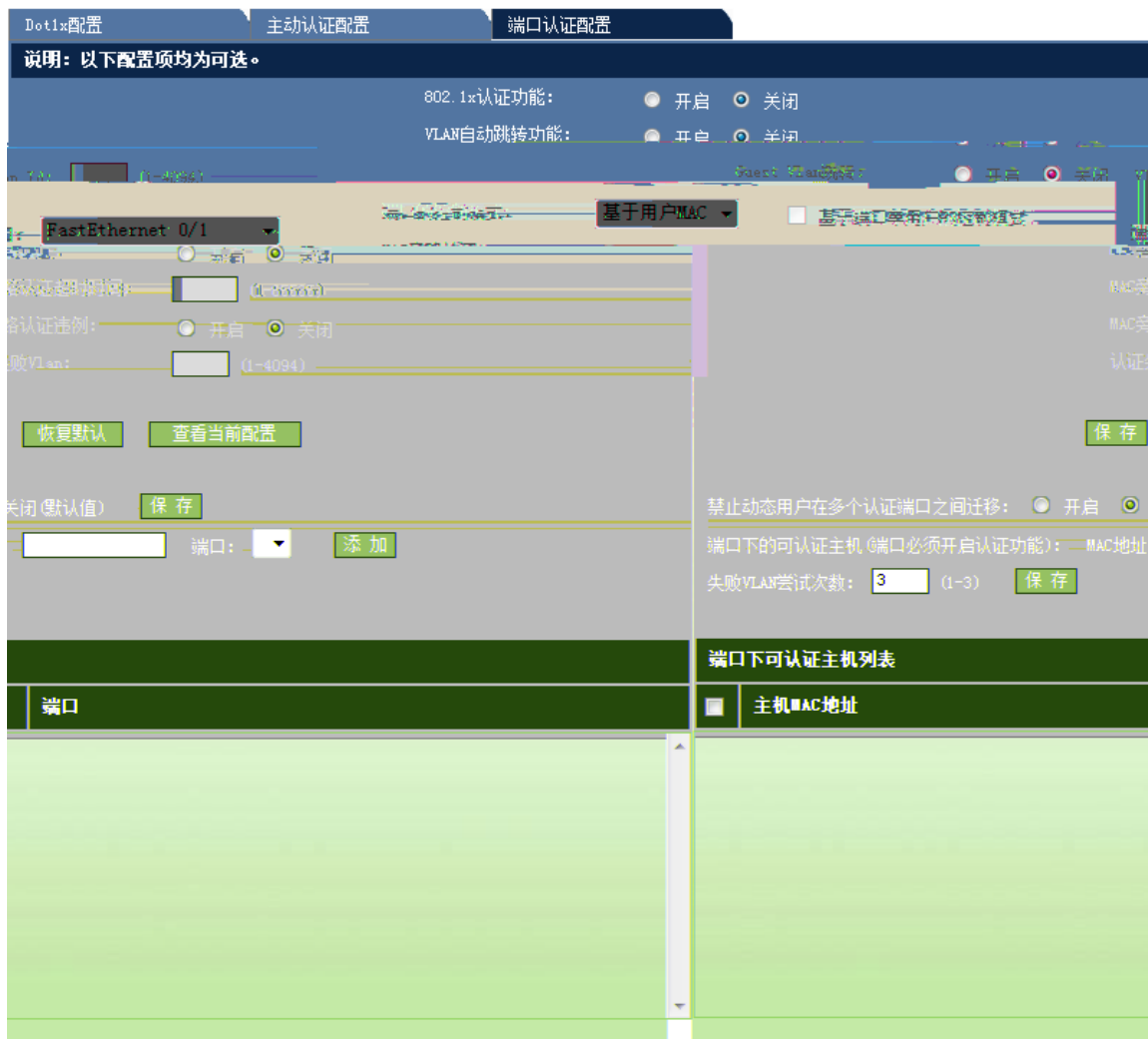
" " " "

" " " "

" " " "

1-62

1



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

802.1x MAC

VLAN " " " "

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
[Table content is obscured by a large redacted area]			

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

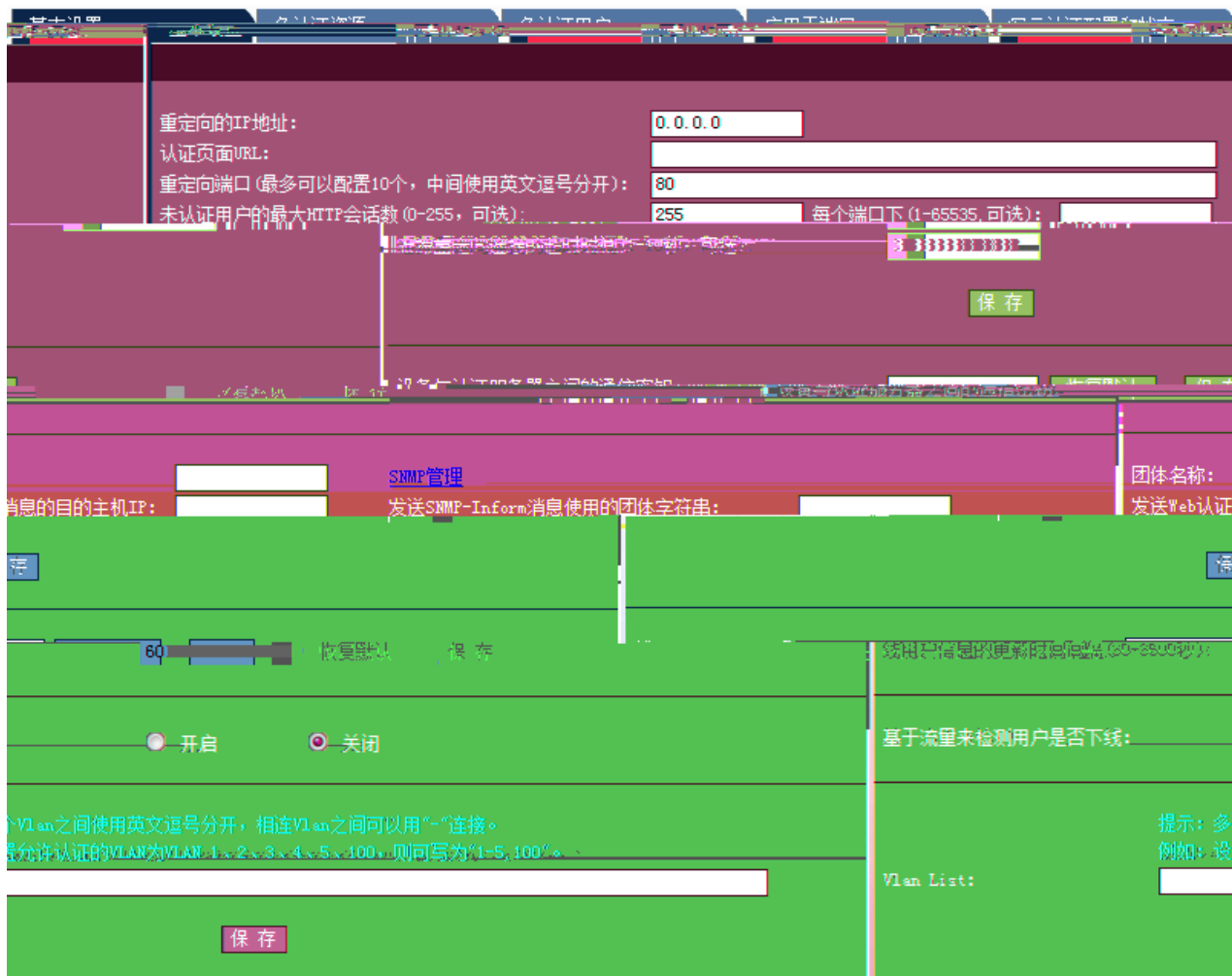
刷新

1.6.13 WEB

" web "

web

1-66 web



web IP URL HTTP (0-255) Web IP

SNMP-Inform , , Vlan List 80



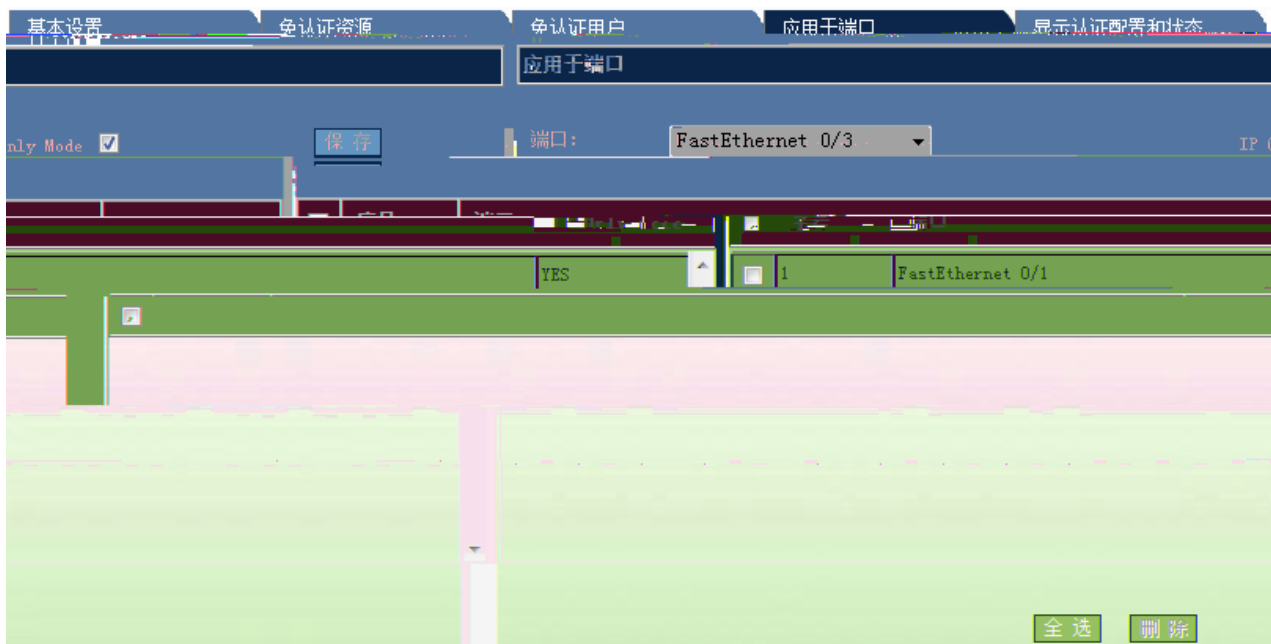
IP

1-68



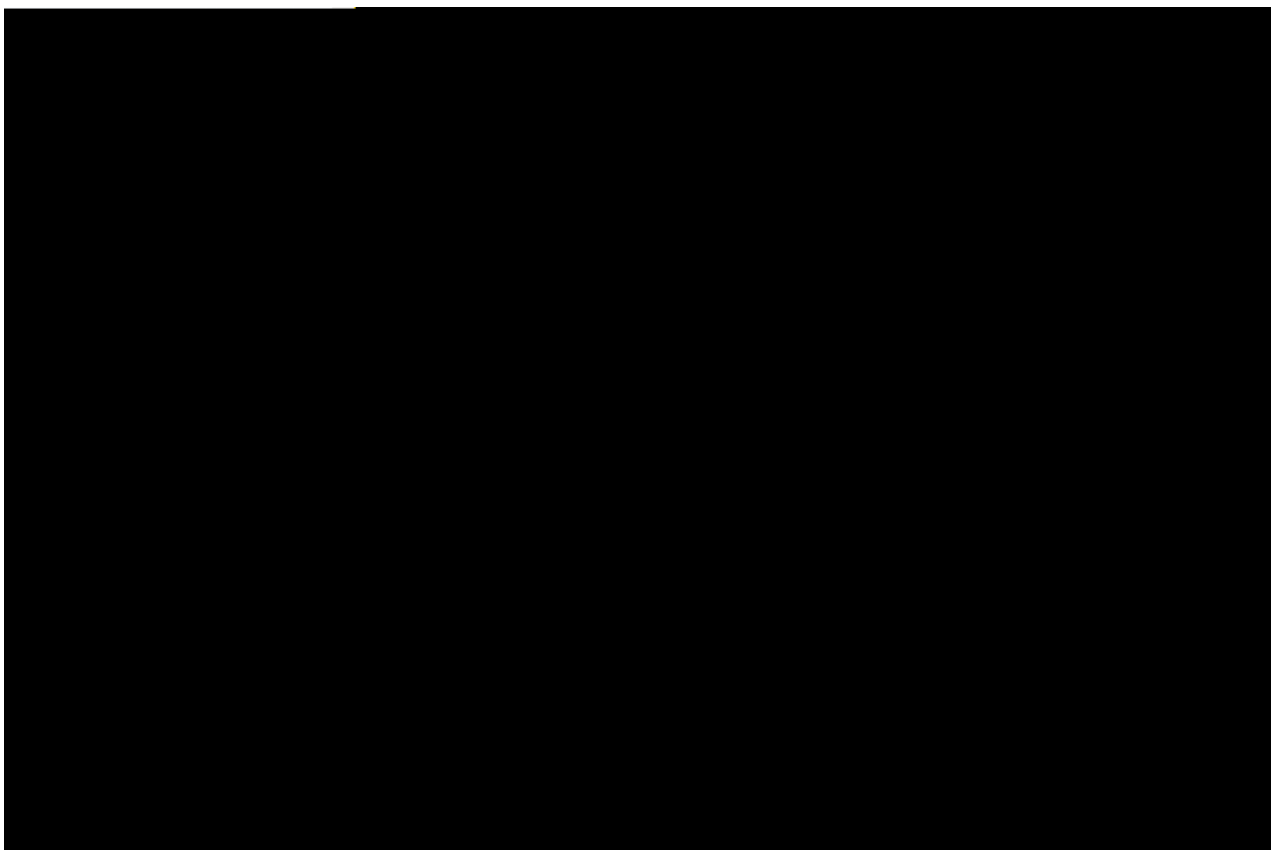
IP

1-69



" "

1-70



IP

1.6.14 DHCP Snooping

“ DHCP Snooping”

DHCP 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。

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
<input type="checkbox"/>			

DHCP Snooping

DHCP Snooping DHCP Snooping MAC

DHCP Snooping

" "

|

1.7 QOS

1.7.1

" "

1-72



ACL " "

1.7.2

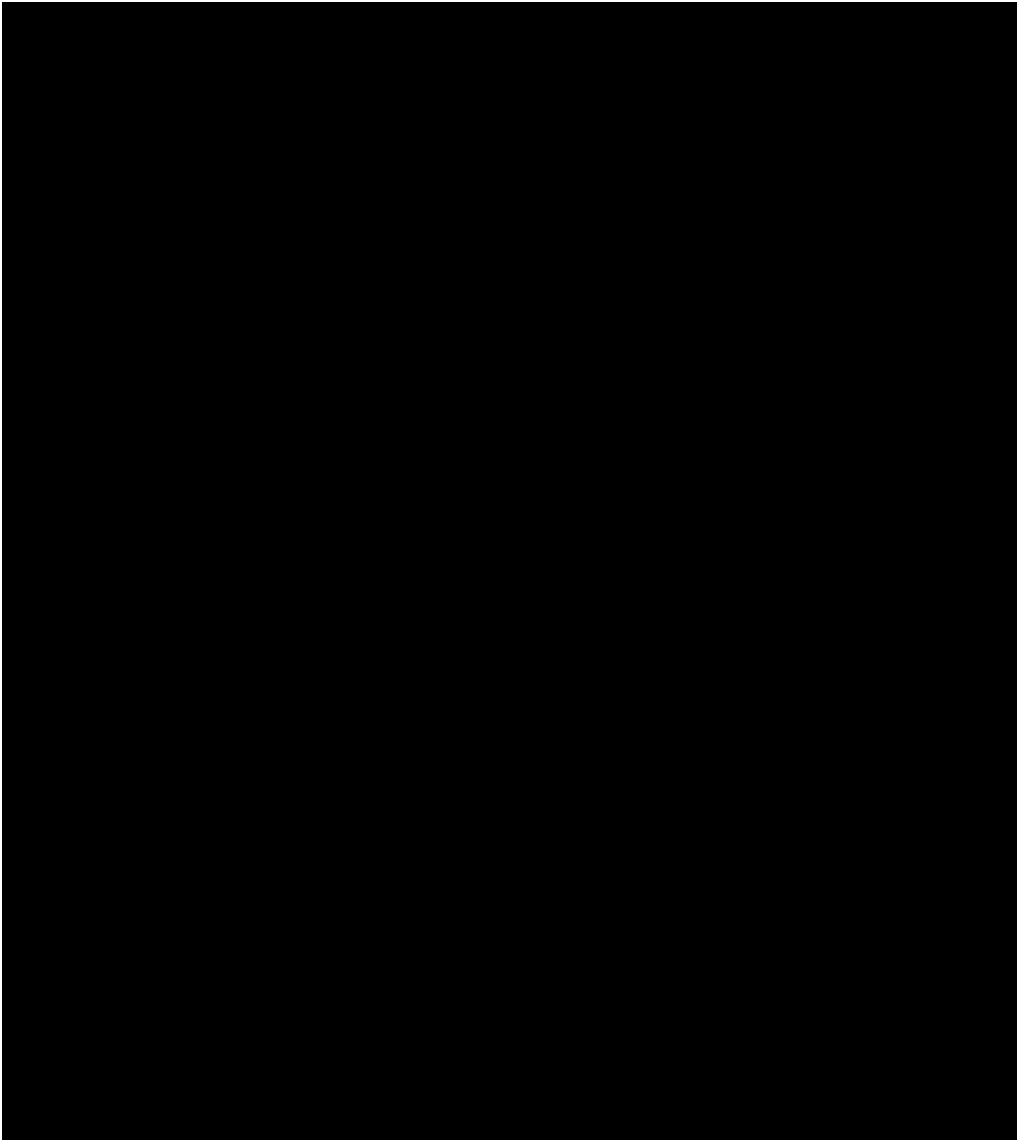
"

&

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

(1-100)

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

" "

1.7.5

" "

1-76



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

" "

端口状态

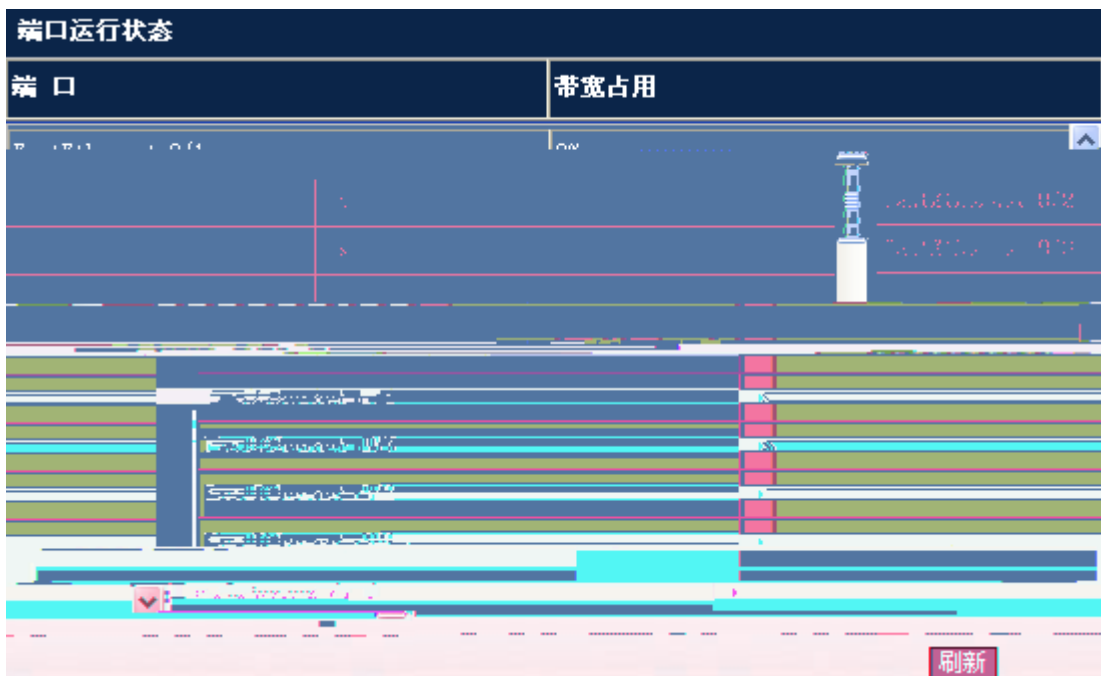
端口	状态	速率	双工	介质	端口名称
down	1	Unknown	Unknown	copper	FastEthernet 0/1
down	2	Unknown	Unknown	copper	FastEthernet 0/2
up	1	Full	100M	copper	FastEthernet 0/3
down	900	Unknown	Unknown	copper	FastEthernet 0/4
down	1	Unknown	Unknown	copper	FastEthernet 0/5
down	1	Unknown	Unknown	copper	FastEthernet 0/6
down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

刷新

1.8.4

“ ”

1-82



1.8.5

“ ”

1-83

```

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
Sysname log messages: disable
Count log messages: disable
Trap logging: level informat
Log Buffer (Total): 4096 Bytes)
ional, 587 message lines logged, 0 fail
have written 4096. Overwritten 2533
can was detected.
can was detected.
can was detected.
can was detected.
can was detected.
Feb 28 06:20:49: %ARP_GUARD-4-SCAN: ARP s
Feb 28 06:33:51: %ARP_GUARD-4-SCAN: ARP s
Feb 28 06:43:52: %ARP_GUARD-4-SCAN: ARP s
Feb 28 06:53:54: %ARP_GUARD-4-SCAN: ARP s
Feb 28 07:03:55: %ARP_GUARD-4-SCAN: ARP s
Feb 28 07:13:57: %ARP_GUARD-4-SCAN: ARP scan was detecte
Feb 28 07:23:59: %ARP_GUARD-4-SCAN: ARP scan was detecte
Feb 28 07:34:00: %ARP_GUARD-4-SCAN: ARP scan was detecte
Feb 28 07:44:01: %ARP_GUARD-4-SCAN: ARP scan was detecte
Feb 28 07:54:03: %ARP_GUARD-4-SCAN: ARP scan was detecte
Feb 28 08:04:04: %ARP_GUARD-4-SCAN: ARP scan was detecte
Feb 28 08:14:06: %ARP_GUARD-4-SCAN: ARP scan was detecte

```

1.9

1.9.1 Ping

* Ping*

Ping

1-85 Ping

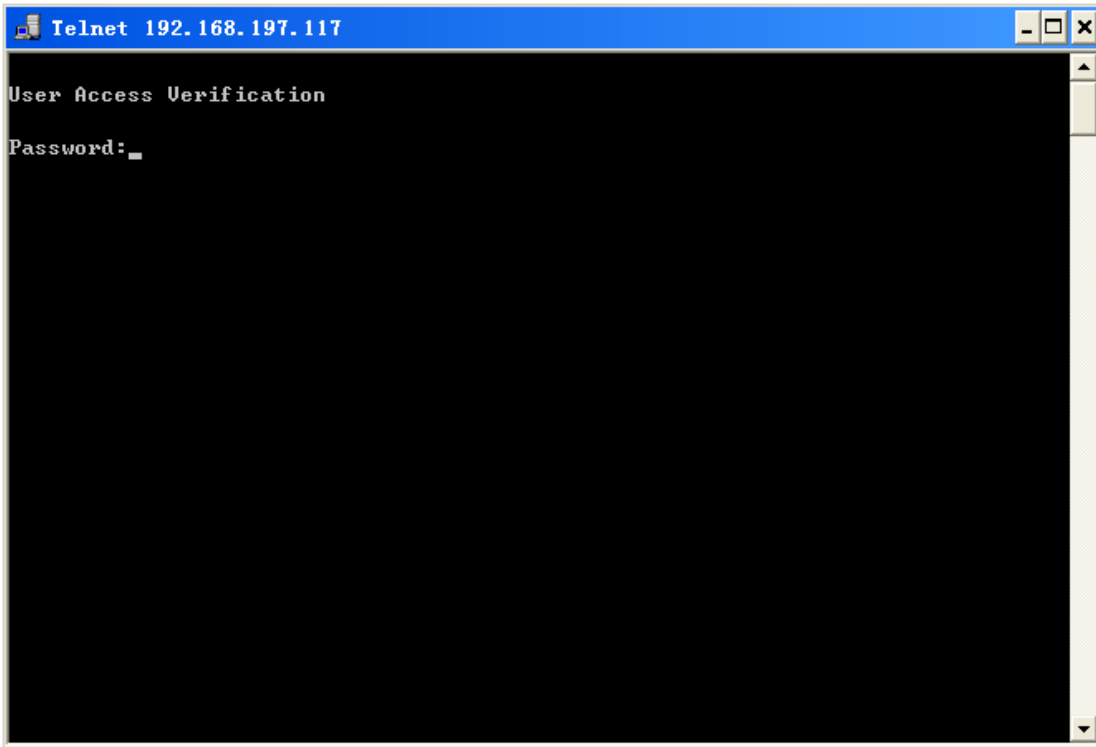


1.9.2 Telnet

" Telnet"

Telnet

1-86 Telnet



" Telnet"

Telnet

PC

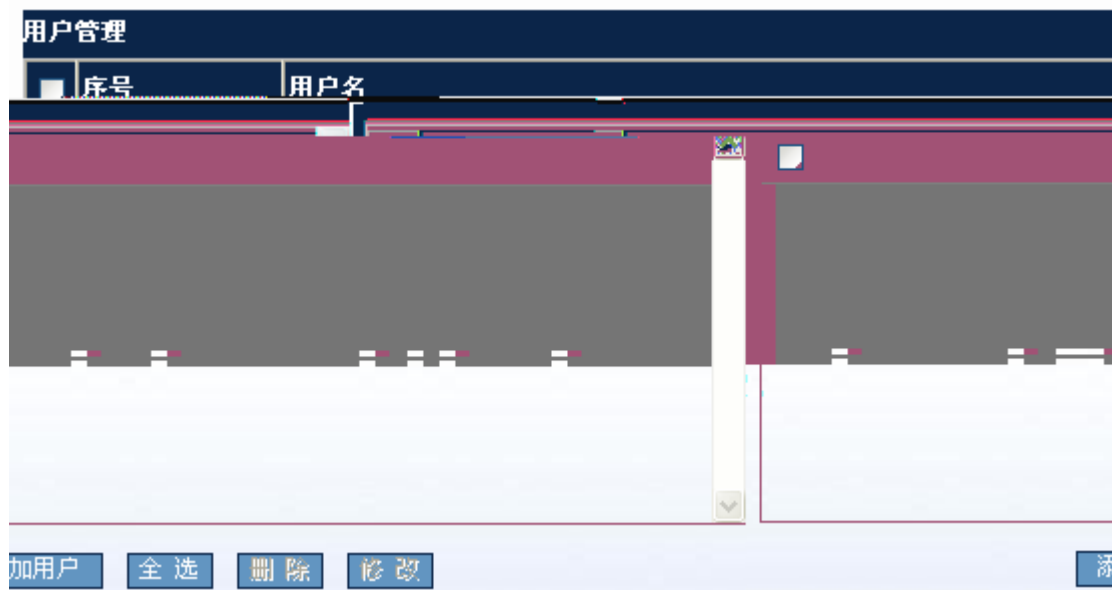
Telnet

PC Telnet

1.9.3

" "

1-87



1-88



1-89



1.9.4

Enable

Enable

1-91



Telnet

Telnet

1.9.5 /

" / "

/

1-92 /

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：

	config.text	TFTP	IP	TFTP	"	"
config.text	TFTP	"	"	TFTP		

1.9.6 WEB

" WEB "

WEB

1-93 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)

	"	"				
IP	192.168.1.1	http://192.168.1.1:8080	"	"	8080	"
	http://192.168.1.1					

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
```

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
```

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