



WEB

RG-AS2T

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)

1 WEB

1.1 WEB

WEB IE
WEB WEB WEB WEB
WEB WEB IE

1.2

1.2.1

WEB WEB WEB PC
IPAD
IE6.0 IE7.0 IE8.0 IE maxthon WEB
1024*768 1280*1024 1440*960

1.2.2

WEB
WEB
IP

1.3 WEB

WEB WEB " WEB "

WEB Enable Enable

1.4 WEB

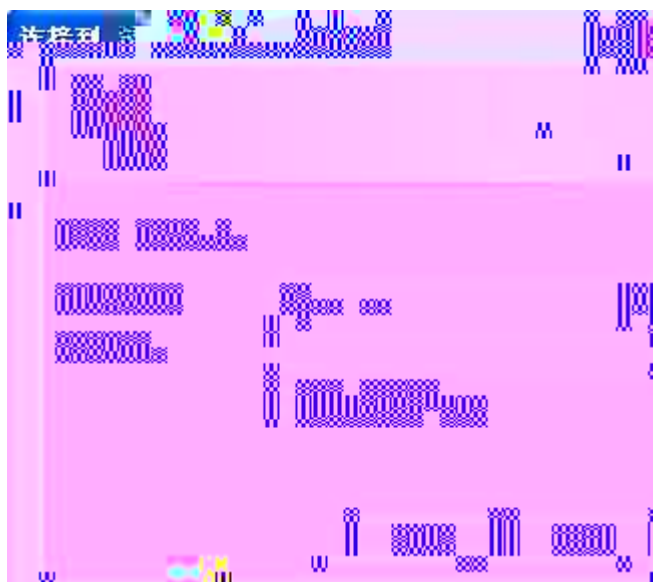
IP IP WEB
IP http://192.168.1.200,

1-1

交换机 WEB 管理平台



1-2



WEB

1-3 WEB



1.5

1.5.1 IP

" IP "

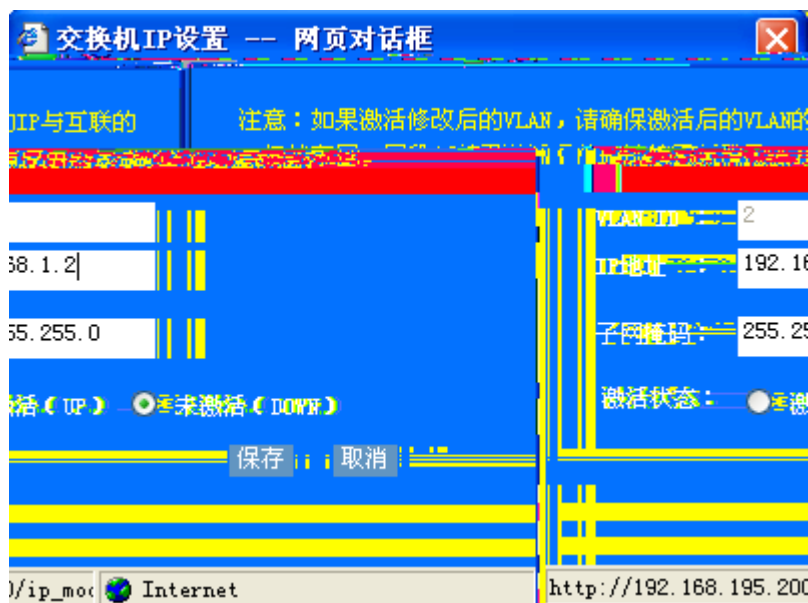
IP

1-4 IP



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划分出多个逻辑子网，同一子网内的用户可以进行二层通讯，不同子网下的用户无法进行二层通讯。

<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

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

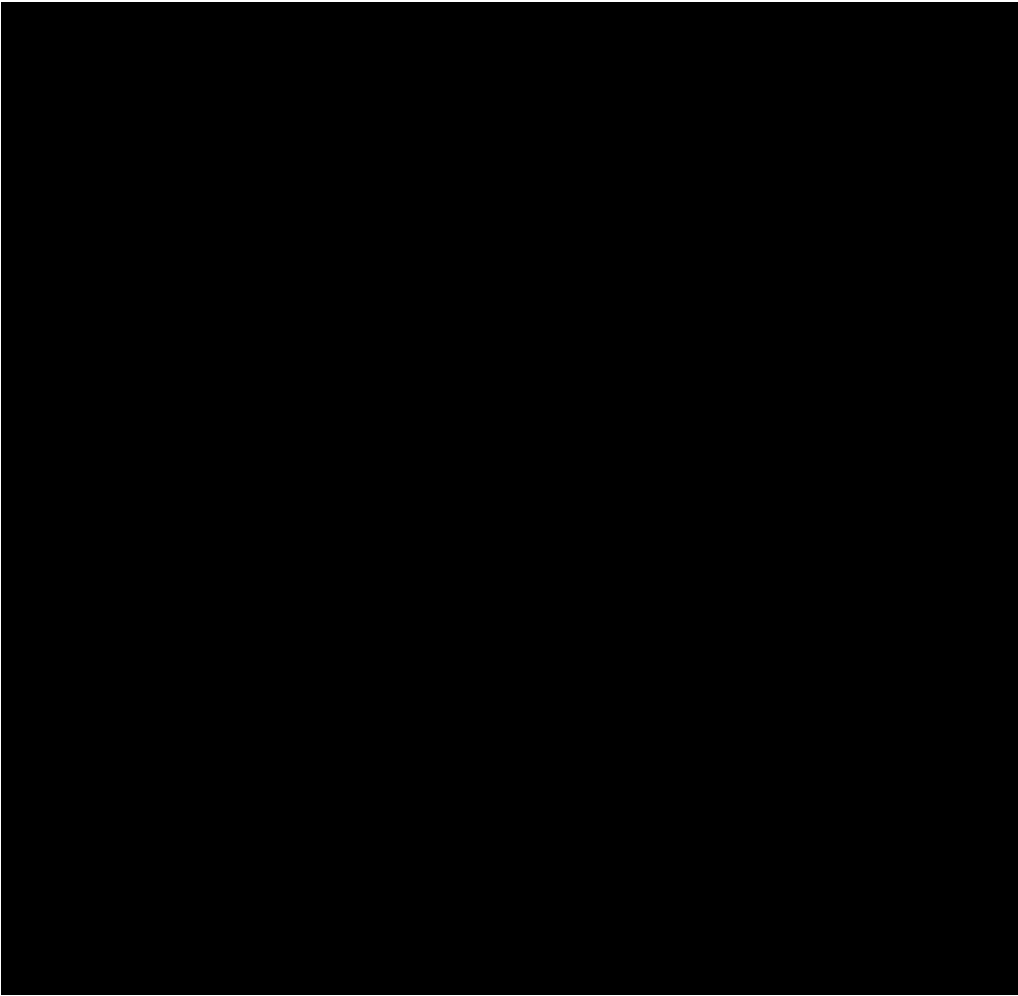
网关设置

说明：网关相当于一个网络连接到另一个网络的“关口”，交换机无法转发的数据包就交给网关处理以便能完成数据包的转发过程。如果网关配置错误，可能导致设备与设备的连接中断。



网关IP地址：





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

聚合端口设置

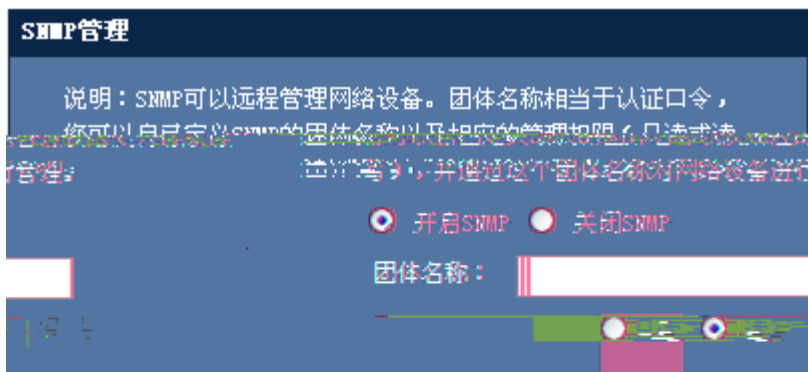
注意：若选择的算法为缺省算法，配置后将不显示。

流量平衡算法选择：

<input type="checkbox"/>	聚合端口	最多成员端口数	二层端口	模式	成员端口

新建 全选 删除

1-17



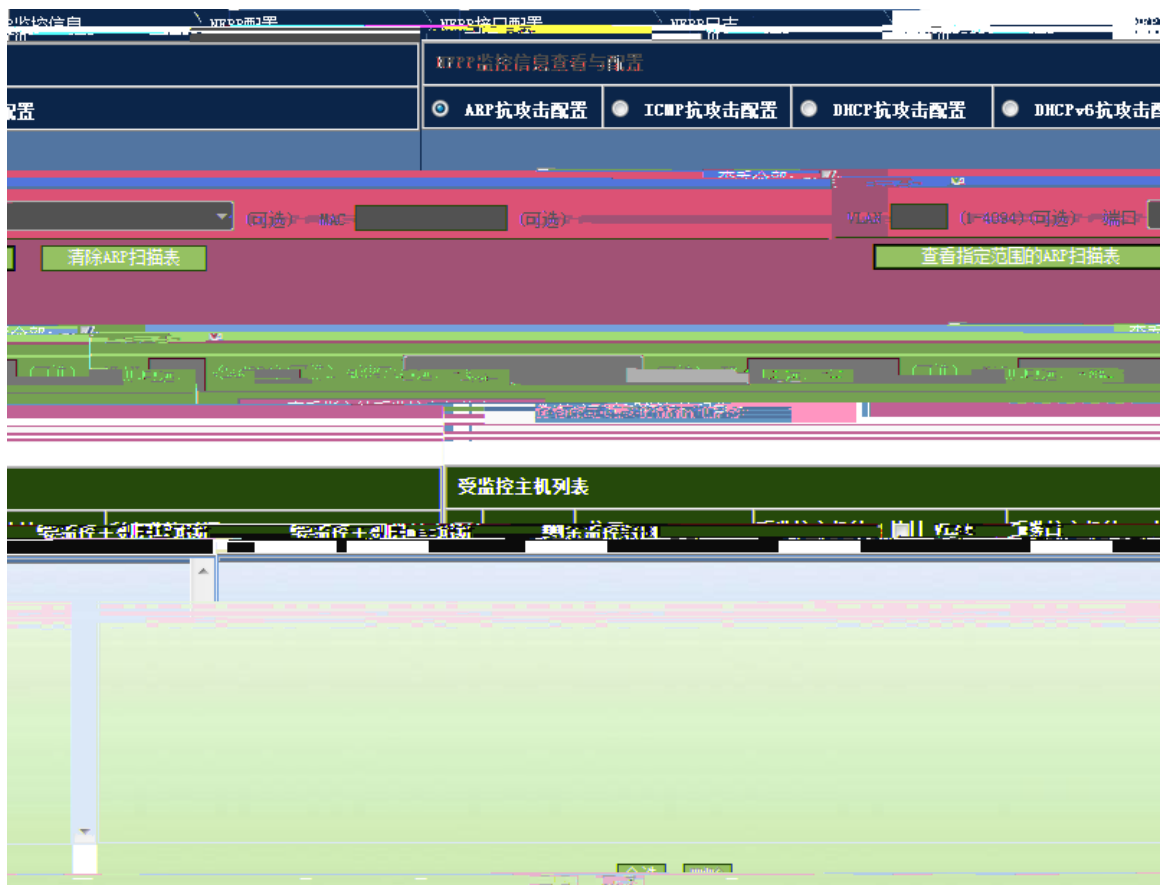
SNMP " SNMP" " SNMP" " "

1.5.13 NFPP

" NFPP "

NFPP

1-23 NFPP



NFPP

1) ARP

1-24 NFPP —ARP

EFPP 监控信息查看与配置

查看全部:

(可选) MAC (可选) VLAN (1-4094) (可选) 端口

删除ARP扫描表 查看指定范围的ARP扫描表

查看全部:

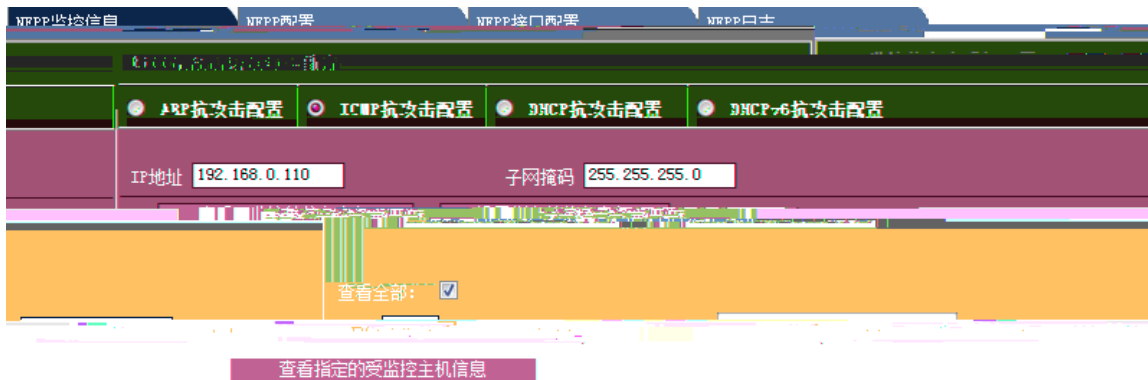
(可选) VLAN (1-4094) (可选) 端口 (可选) IP (可选) MAC (可选) (可

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
-	-	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 11:21:24	Fa0/40
-	-	001a.a942.f27f	2016-6-6 11:22:24	Fa0/40
-	-	001a.a942.f27f	2016-6-6 11:23:25	Fa0/40
-	Fa0/40	-	001a.a942.f27f	2016-6-6 11:25:34

ARP

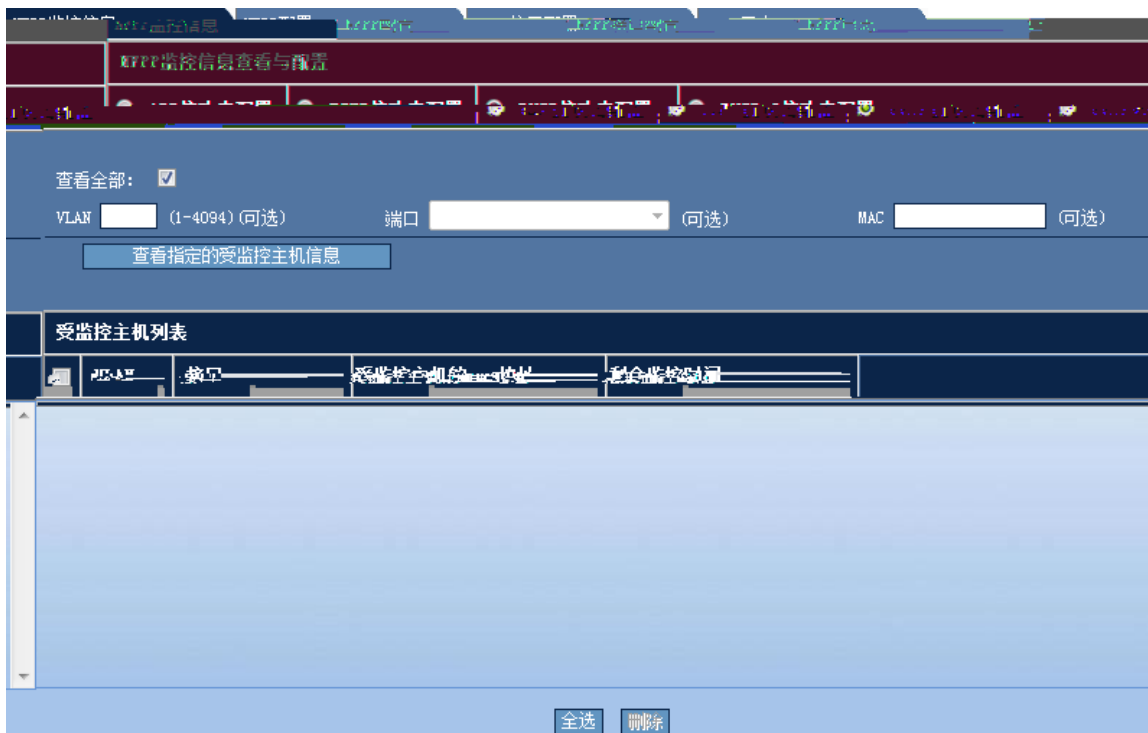
ARP



ICMP					
		IP			

3) DHCP

1-26 NFPP —DHCP



DHCP

4) DHCPv6

1-27 NFPP —DHCPv6



DHCPv6

NFPP

1-28 NFPP



1) CPU

1-29 CPU

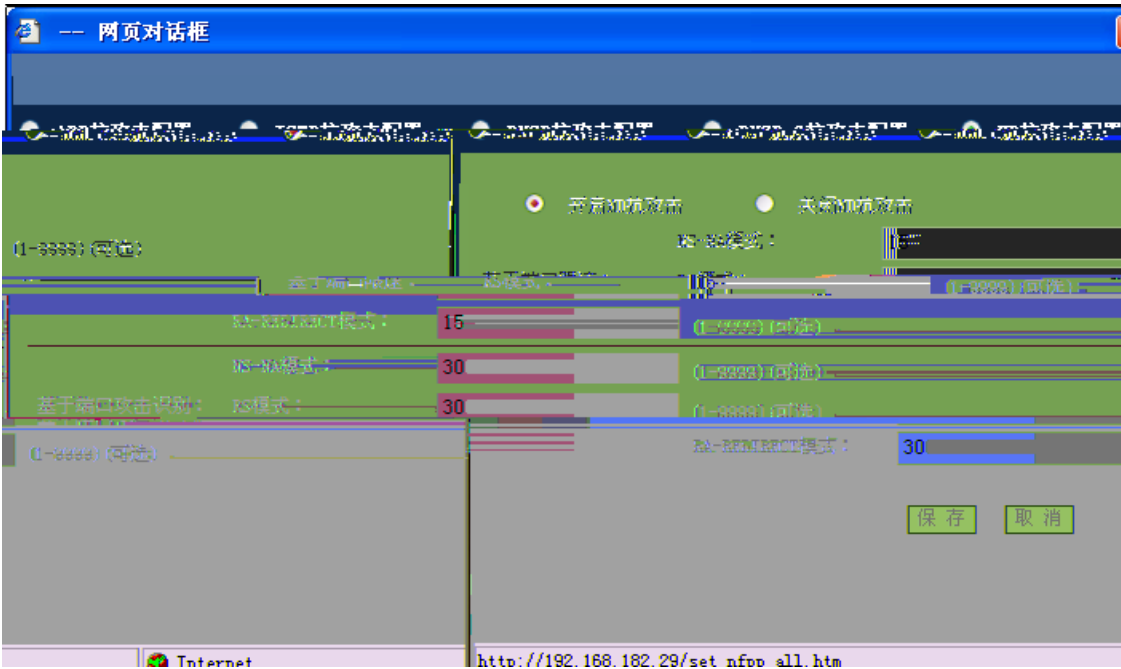


CPU

" "

2) NFPP

1-30 NFPP



NFPP

" "

NFPP

" "

NFPP

NFPP

1) ARP

1-31 NFPP

—NFPP

ARP

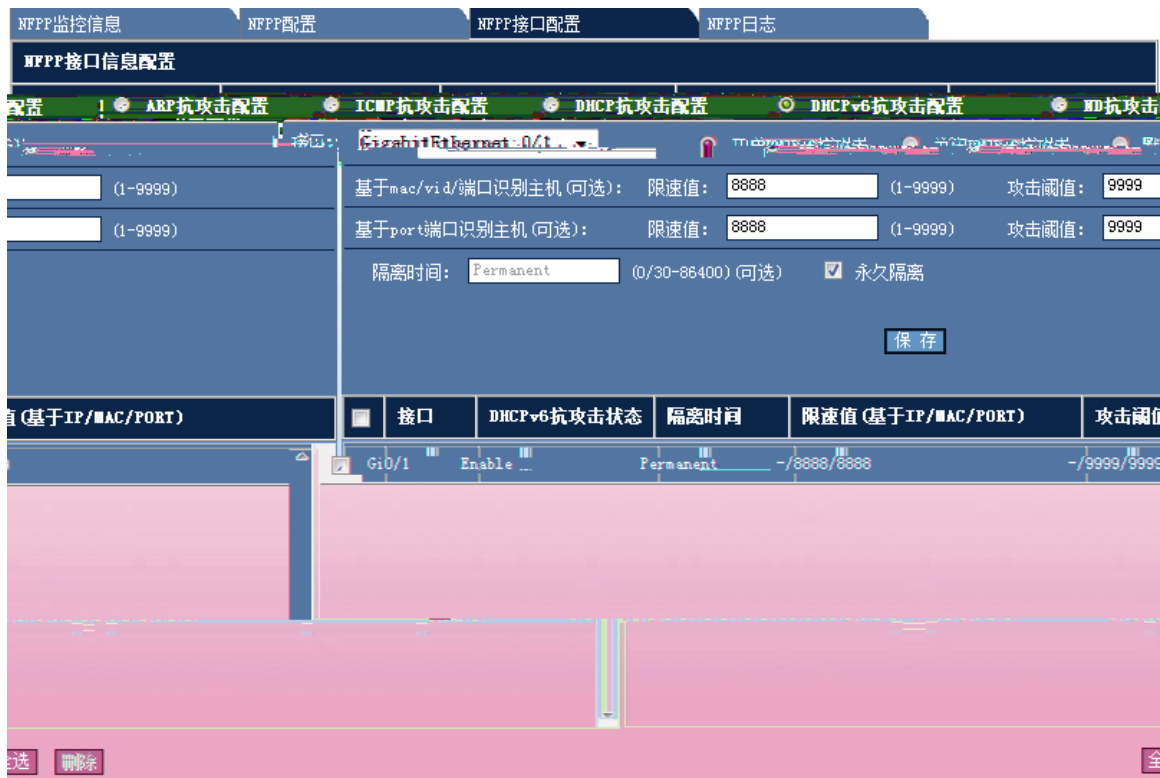


ARP NFPP

" "

2) ICMP

1-32 NFPP —NFPP ICMP



DHCPv6

NFPF

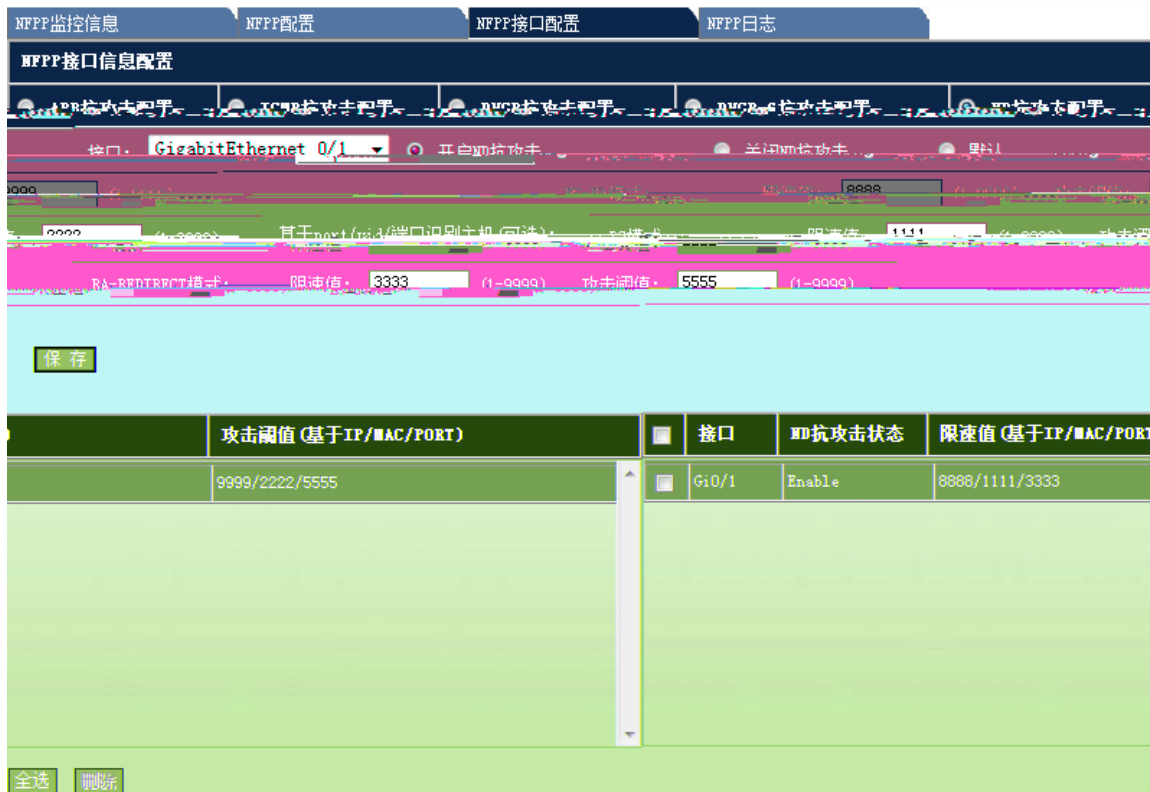
" "

5) ND

1-35 NFPF

—NFPF

ND



ND NFPP " "

NFPP

1-36 NFPP



NFPP

" "

" "

" "

1-37

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)

用 (连接): (1-4094) (可选) 指定需要记录日志的IP地址(用), (例外: 相应的区域可)

ernet 0/1 指定需要记录日志的端口 (可选):

ernet 0/2

ernet 0/3

日志缓冲区:

Protocol	VLAN	Interface	IP address	MAC address	Reason	Timestamp

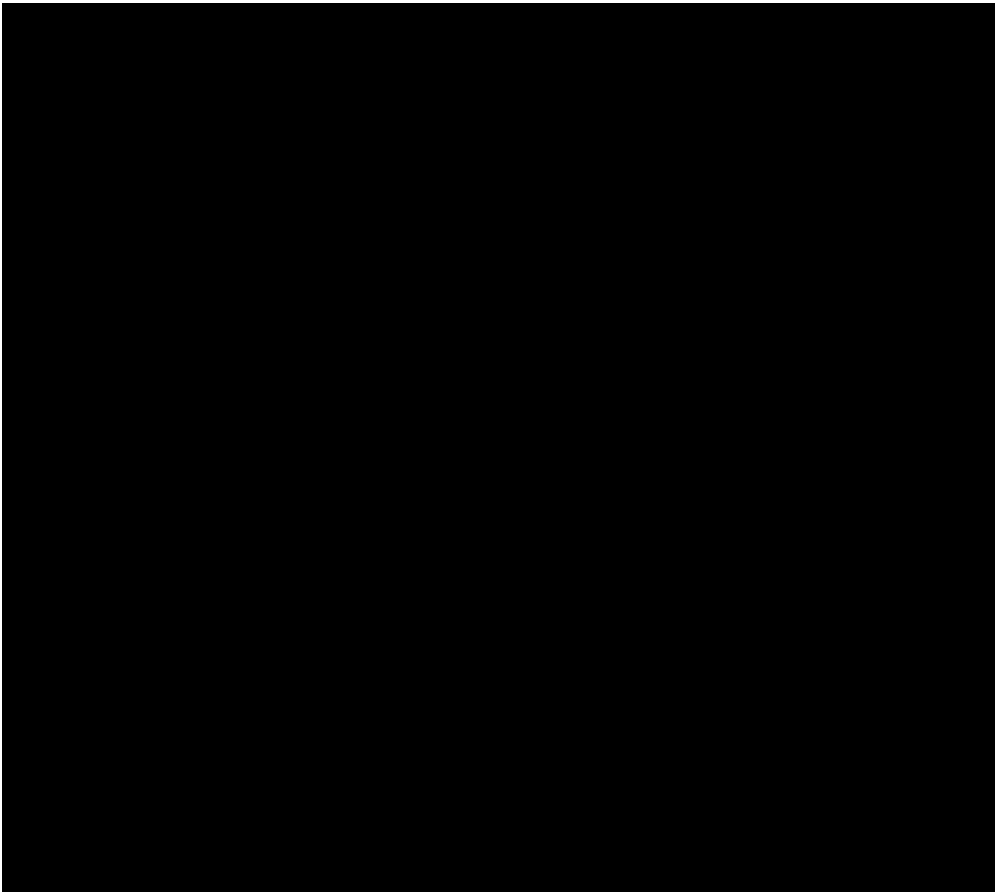
1.6

1.6.1 ARP

" ARP "

ARP

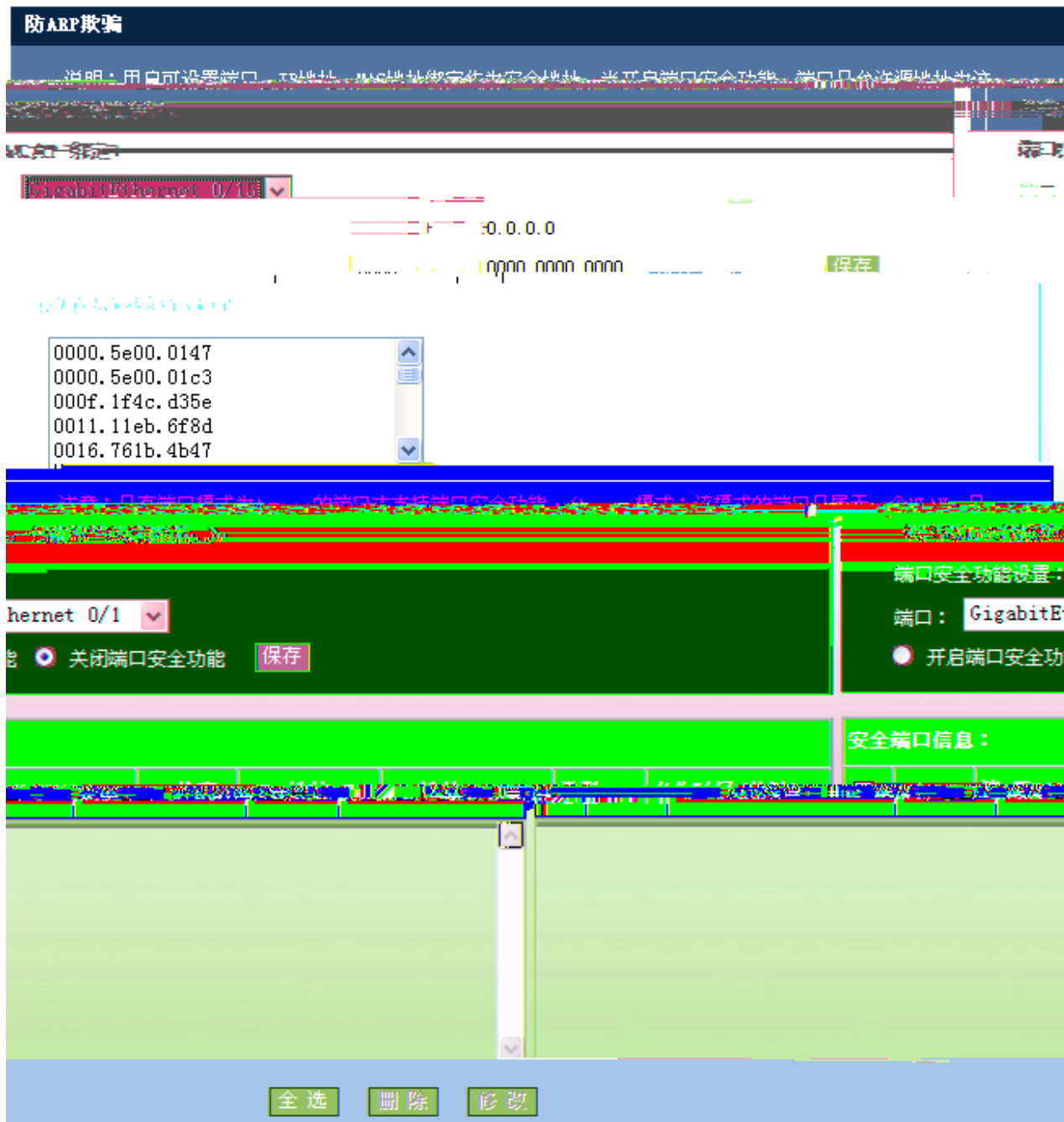
1-38 ARP



" "

" "

1.6.2 ARP



/MAC/IP

/MAC/IP

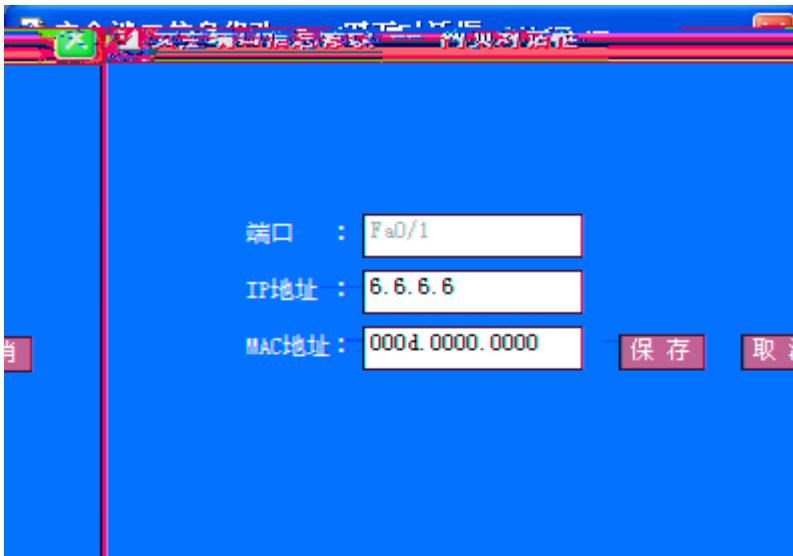
IP MAC " "

MAC

GigabitEthernet 0/15

MAC

1-40



显示ACL信息 **ACL配置** 将ACL应用于端口

ACL配置

ACL配置向导

1. 配置ACL规则

2. 配置ACL应用

被忽略：通配符掩码中的“1”表示忽略IP地址中对应的位，而“0”则表示该位必须保留。如果忽略了通配符掩码，0.0.0.0将被认为是缺省的屏蔽字。

配置标准IP访问列表 配置扩展IP访问列表

规则 : **禁止** ▼

列表 ID (名称): (1-99) (1300-1999)

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)

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）

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。（编号为100-269、2700-2699）

IPv6标准访问控制列表：根据数据流的源IPv6地址制定匹配条件。（编号为1-99）

IPv6扩展访问控制列表：根据数据流的源IPv6地址、源端口、目的IPv6地址、目的端口制定匹配条件。（编号为100-269、2700-2699）

在配置ACL时，请根据数据流的源IP地址、源端口、目的IP地址、目的端口制定匹配条件。如果忽略了通配符掩码，0.0.0.0将被认为是设备的屏蔽符。

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 : TC

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)

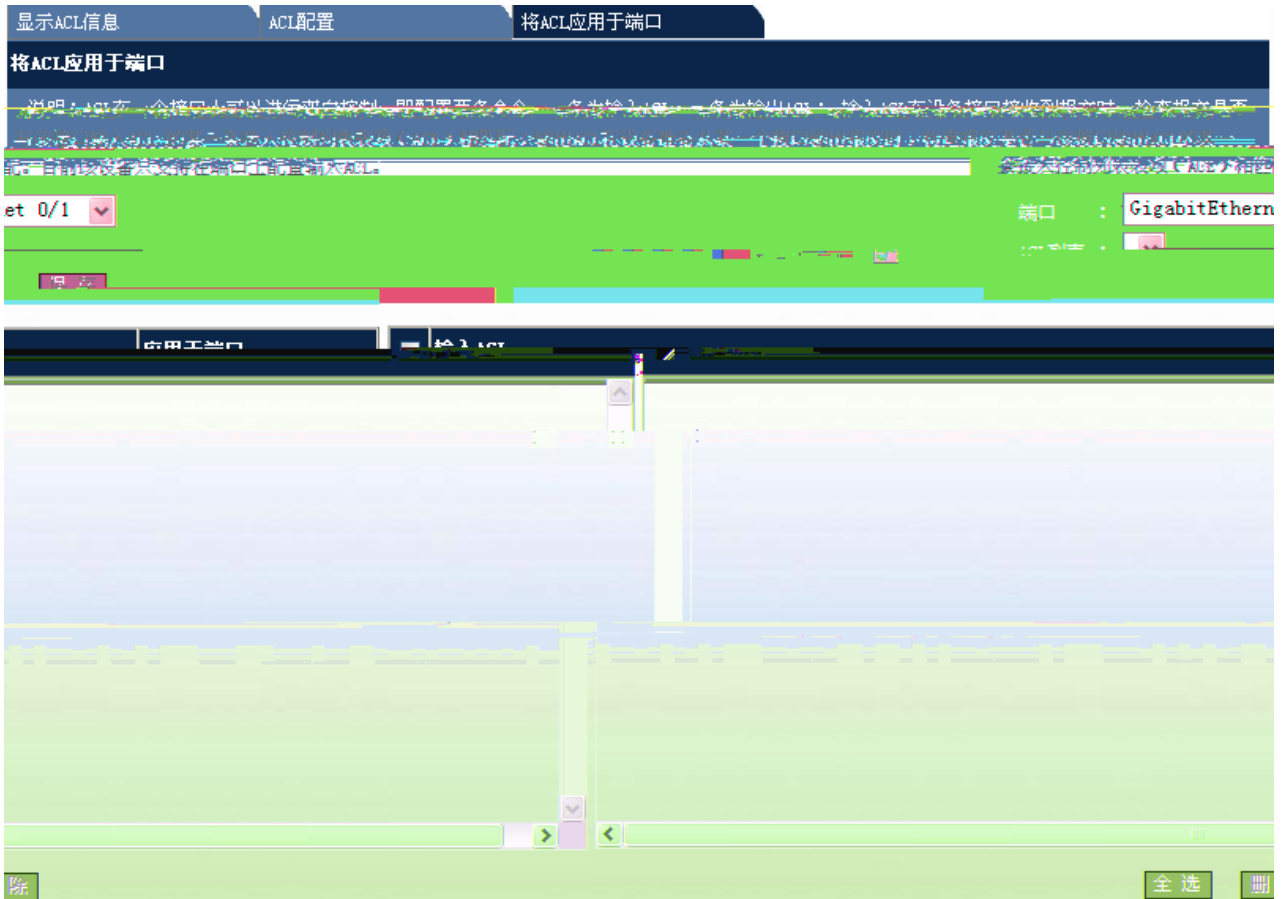
目的IP地址 : ● 任意目的IP地址
● 指定IP地址范围： 0.0.0.0 通配符掩码： (可选)

目的端口 : (1-65535) (可选)

保存

ID

TCP



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

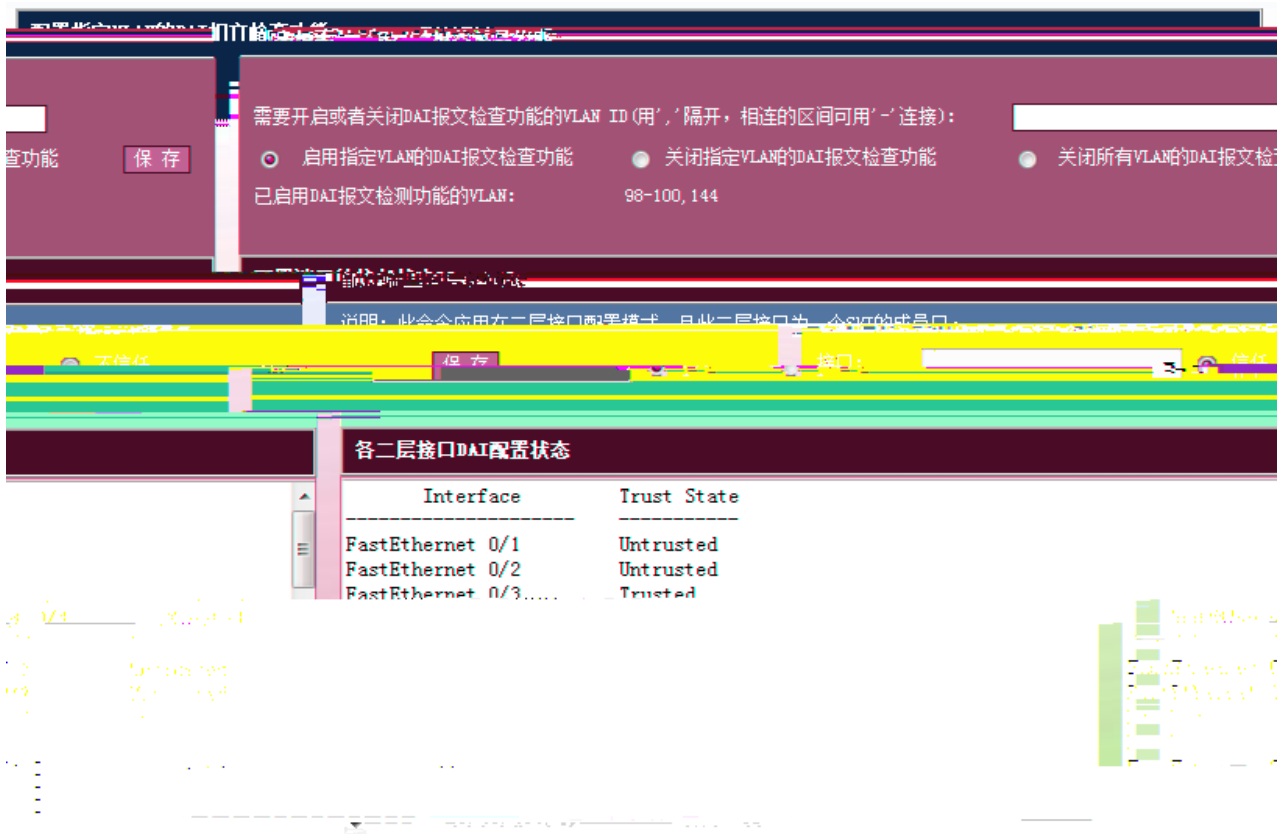
IP+MAC

"

IP+MAC

()"

IP



VLAN DAI

VLAN DAI

VLAN 100 DAI vlan-id 100 ARP DAI

" DAI VLAN ID" VLAN

VLAN DAI VLAN DAI " "

DAI VLAN

ARP ARP DAI

ARP ARP DAI

" " " " " "

" DAI "

1.6.7 GSN

" GSN"

GSN

1-49 GSN



GSN

GSN

GSN

GSN

GSN

SMP server

SMP server

v1

v2 v3

Community User

" "

" "

GSN

GSN

" "

" "

1.6.8 CPP

" CPP "

CPP

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

The screenshot displays a web interface for configuring AAA parameters and Radius server groups. The top section, titled "AAA参数配置", includes options for "AAA new-model" (radio buttons for "开启" and "关闭"), a "密钥" (password) field with a "隐藏密钥" dropdown, and checkboxes for "记帐计费更新功能" and "非锐捷认证服务器动态acl下发". The "IP授权模式" is set to "disable". The bottom section, titled "Radius服务器组", shows a "组名" field and "正端口" and "帐端口" fields, both with "(0-65536) (可选)" ranges. A terminal window at the bottom shows the configuration for a "Radius group radius" with parameters: Vrf: not-set, Server: 7::1 (Auth: 1812, Acc: 1813, State: Active) and Server: ::1 (Auth: 1812).

RADIUS IP

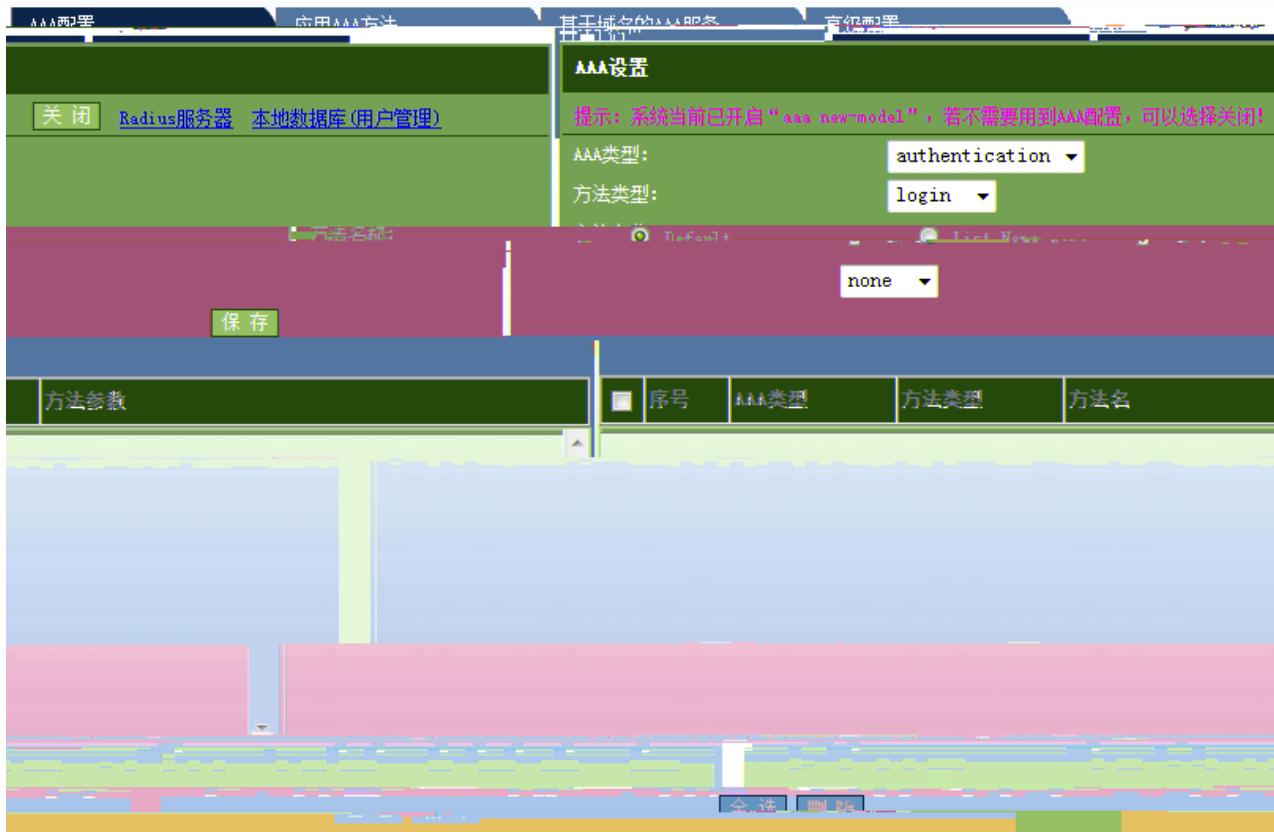
Radius

1.6.10 AAA

" AAA "

AAA

1-56 AAA



AAA

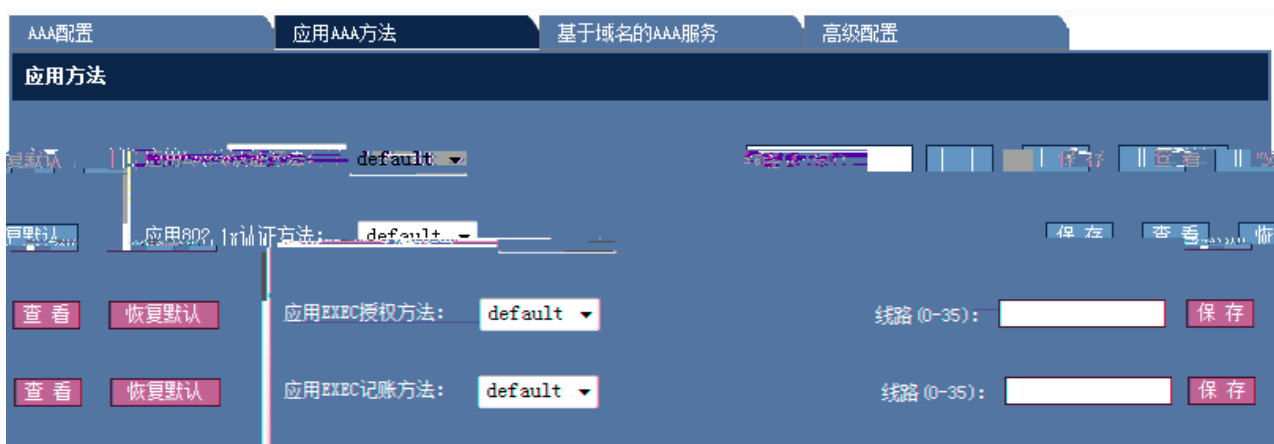
```

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

```

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

Default Domain Name

default default

default default

default default

默认: Dot1x认证方法: PPP认证方法: 授权方法(network): 记账方法(network):

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

AAA配置 应用AAA方法 基于域名的AAA服务 高级配置

监视AAA用户

当前AAA用户:

配置支持VRF的AAA组

RADIUS服务器组名: VRF名:

用户认证失败锁定

login登录用户尝试失败次数 (1-2147483647):

生成认证失败的时间 (0-3600000):

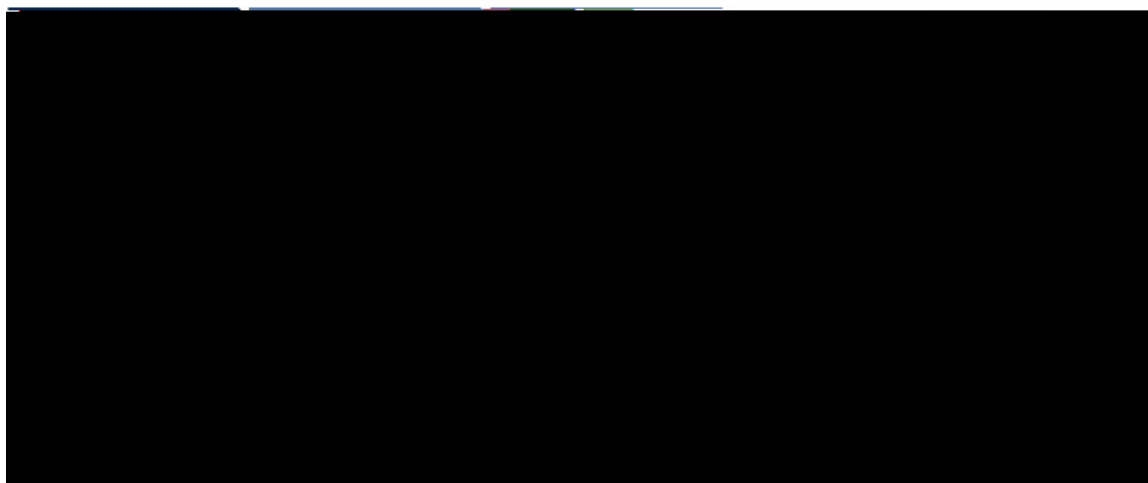
Name	Tries	Lock	Timeout(min)
AAA	AAA	VRF	AAA

1.6.11 Dot1x

" Dot1x "

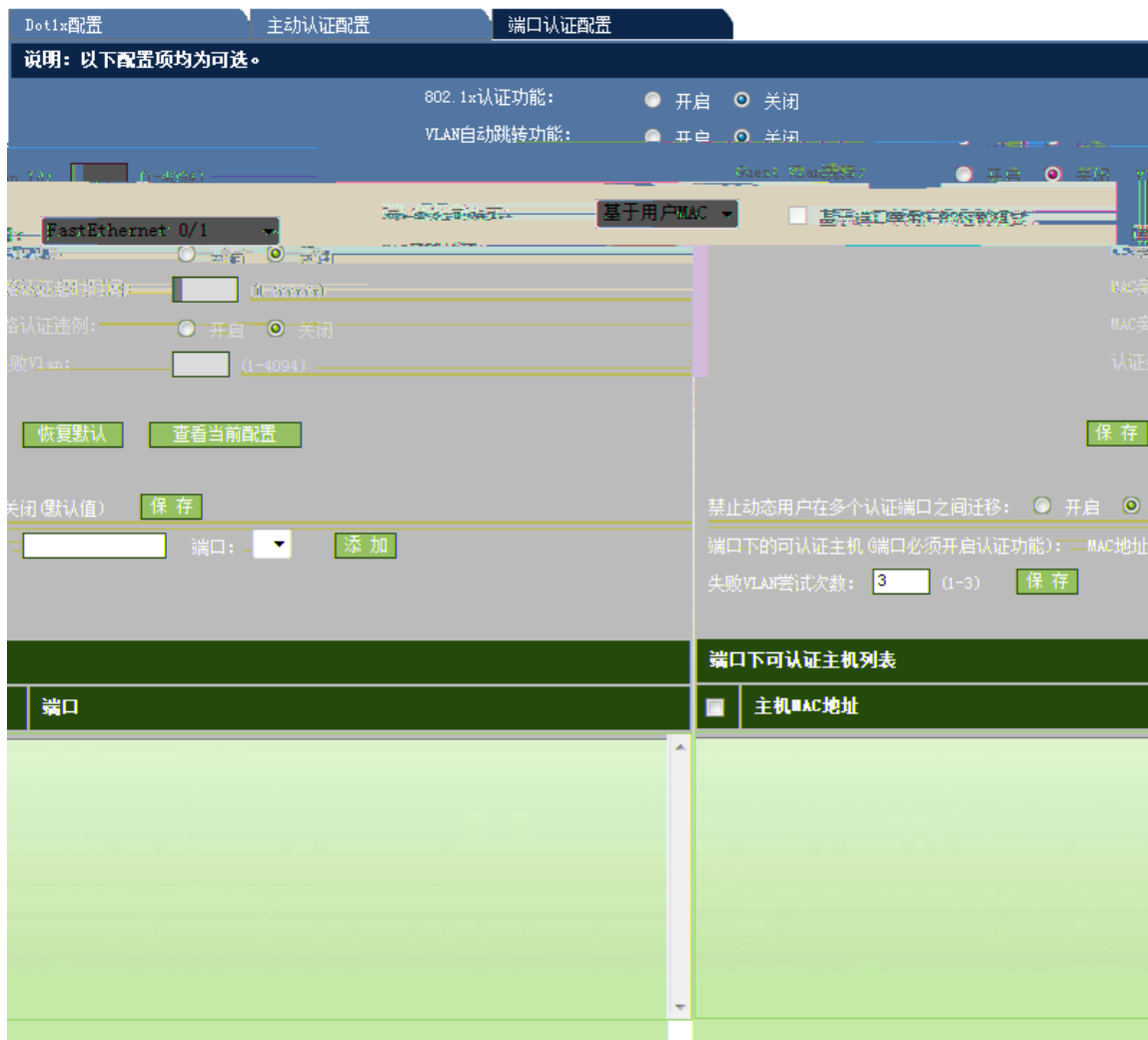
Dot1x

1-60 Dot1x



Dot1x

Dot1x



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 pink watermark]			

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...0...70...	1	绑定
4	192.168.23.70	001...0...70...	1	绑定
5	192.168.23.76	001...0...70...	5	绑定
6	192.168.23.81	001...0...70...	5	绑定
7	192.168.23.84	001...0...70...	5	绑定

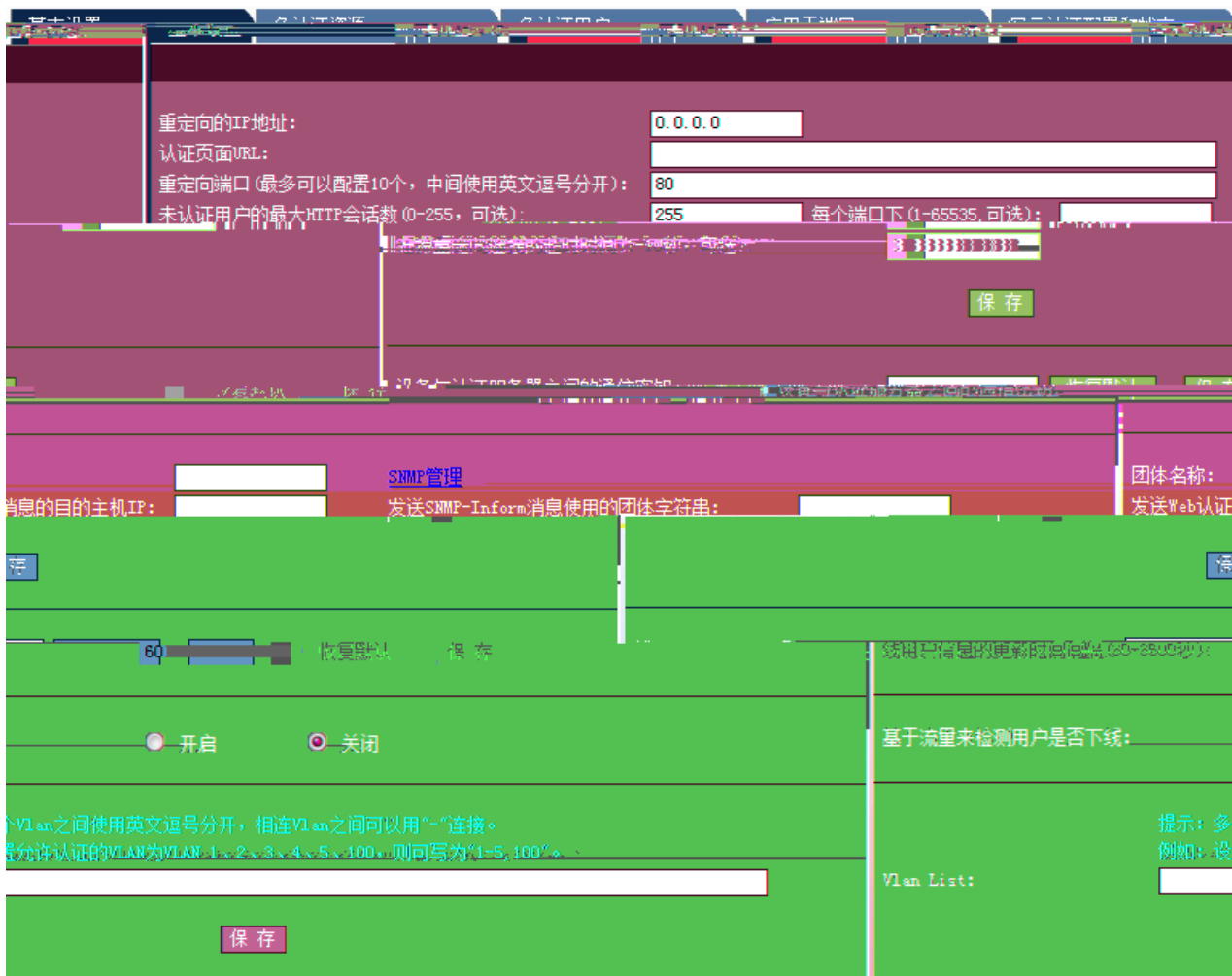
刷新

1.6.13 WEB

" web "

web

1-66 web



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



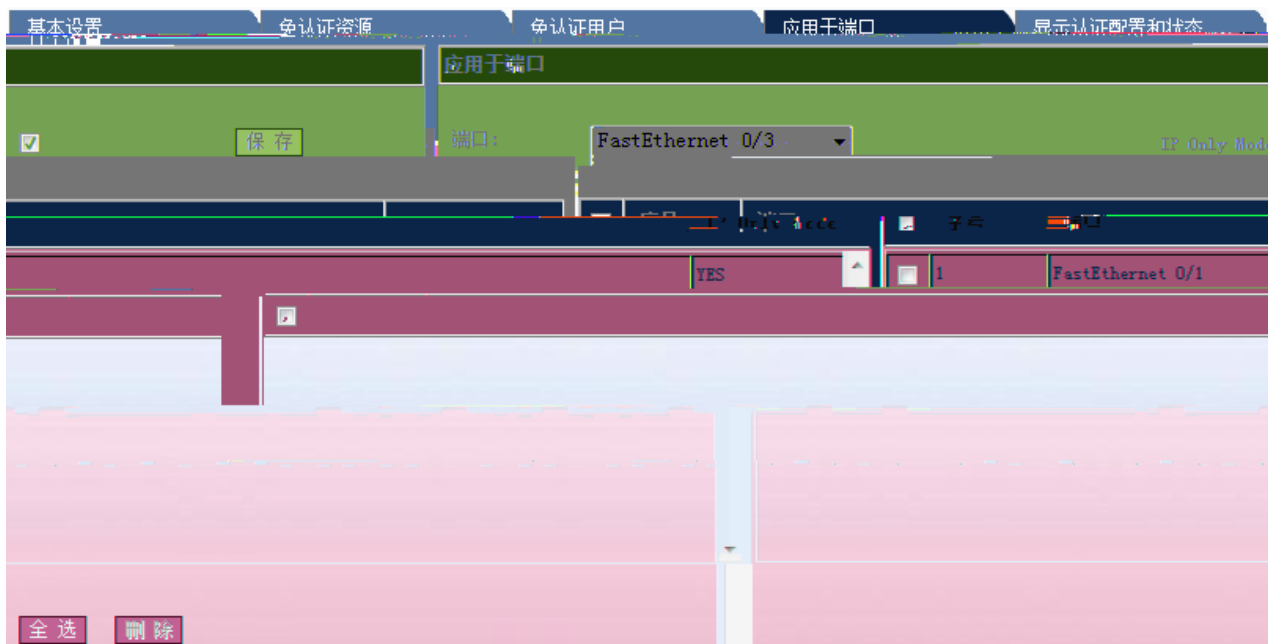
IP

1-68



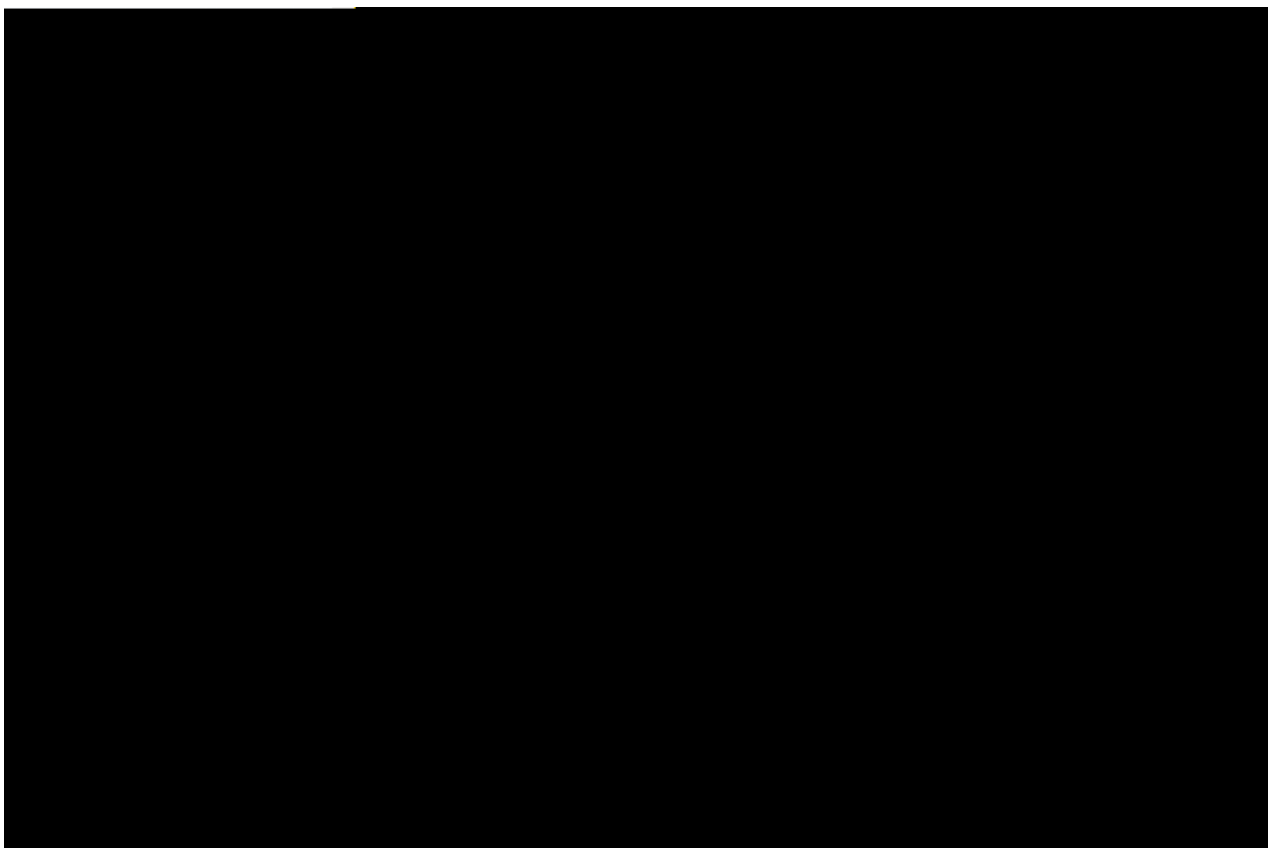
IP

1-69



" "

1-70



IP

1.6.14 DHCP Snooping

“ DHCP Snooping”

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。

保存

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： 保存

DHCP Snooping配置信息

■	端口	信任端口	限速
<div style="border: 1px solid #ccc; width: 20px; height: 20px; margin: 0 auto;"></div>			

全选
删除

DHCP Snooping

DHCP Snooping DHCP Snooping MAC " "

DHCP Snooping

" "

" "

1.7 QOS

1.7.1

" "

1-72



ACL " "

1.7.2

1-73

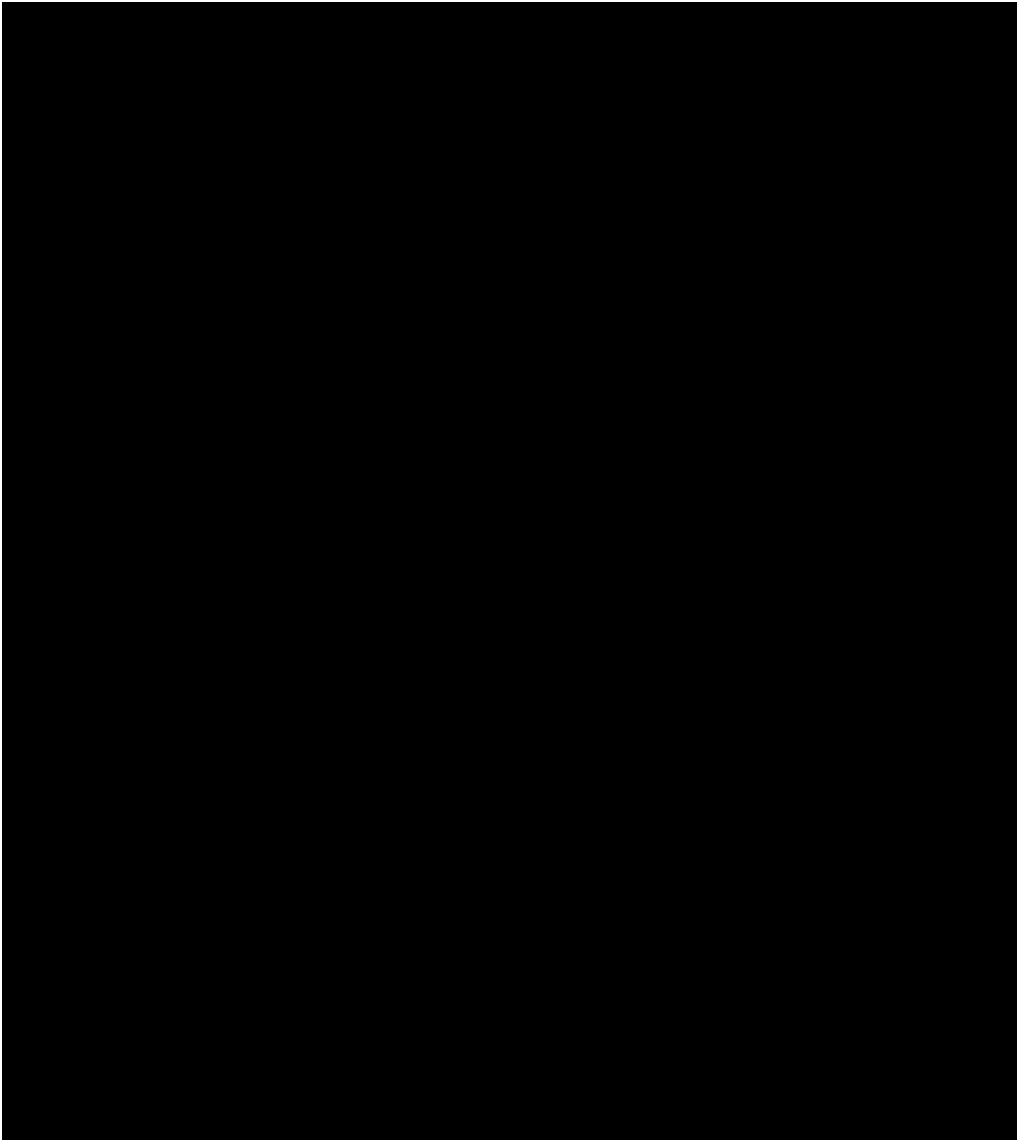


DSCP

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

多播

单播

抑制级别:

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

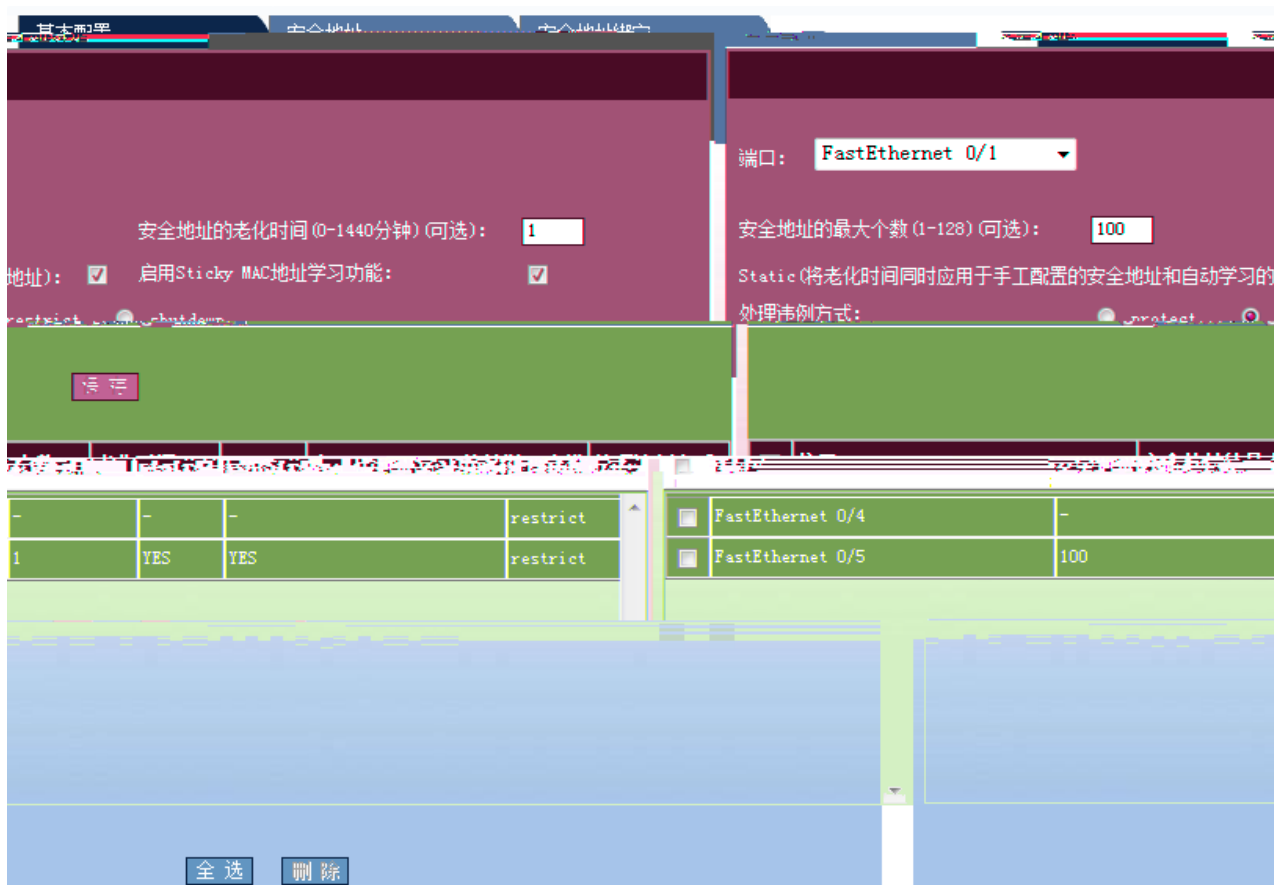
" "

" "

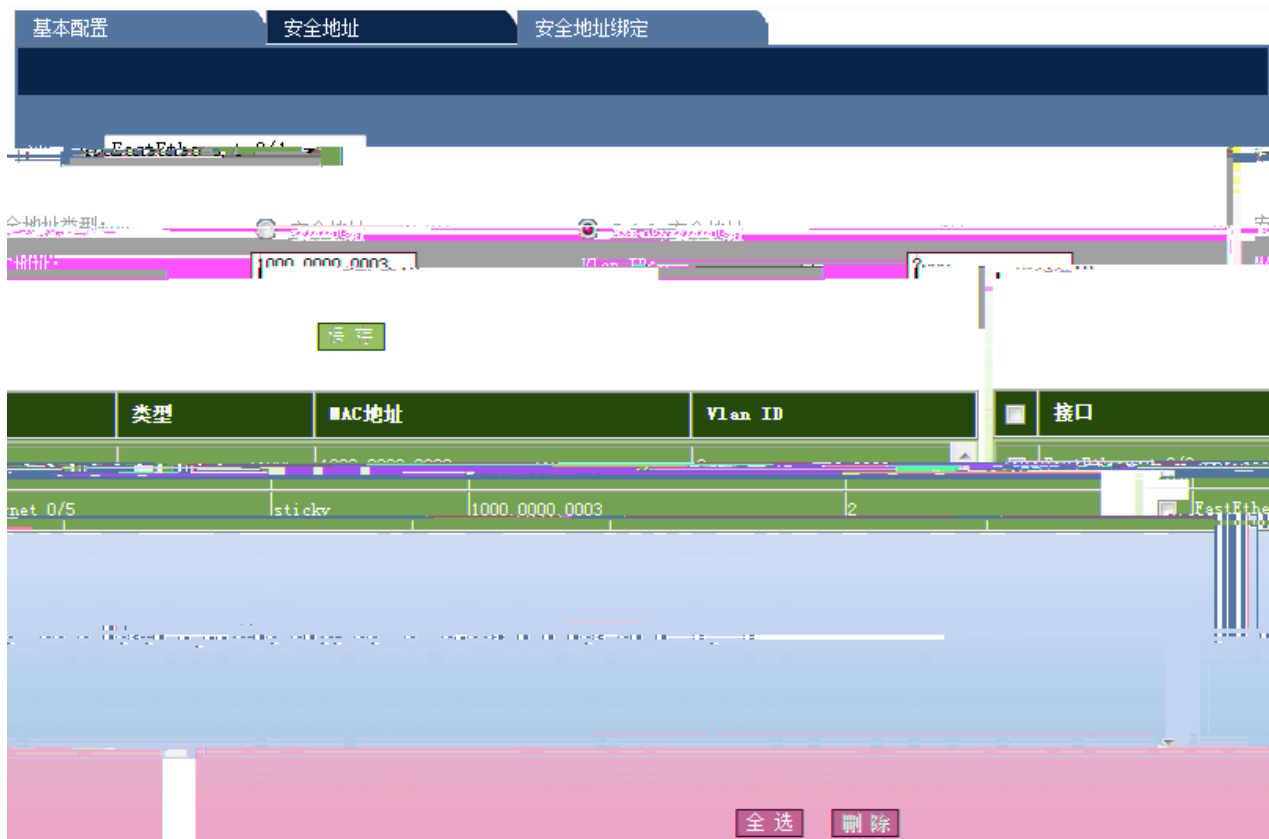
1.7.5

" "

1-76



Static Sticky Mac



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 " "

IP MAC Vlan

" "

1.8

1.8.1

" "

端口状态

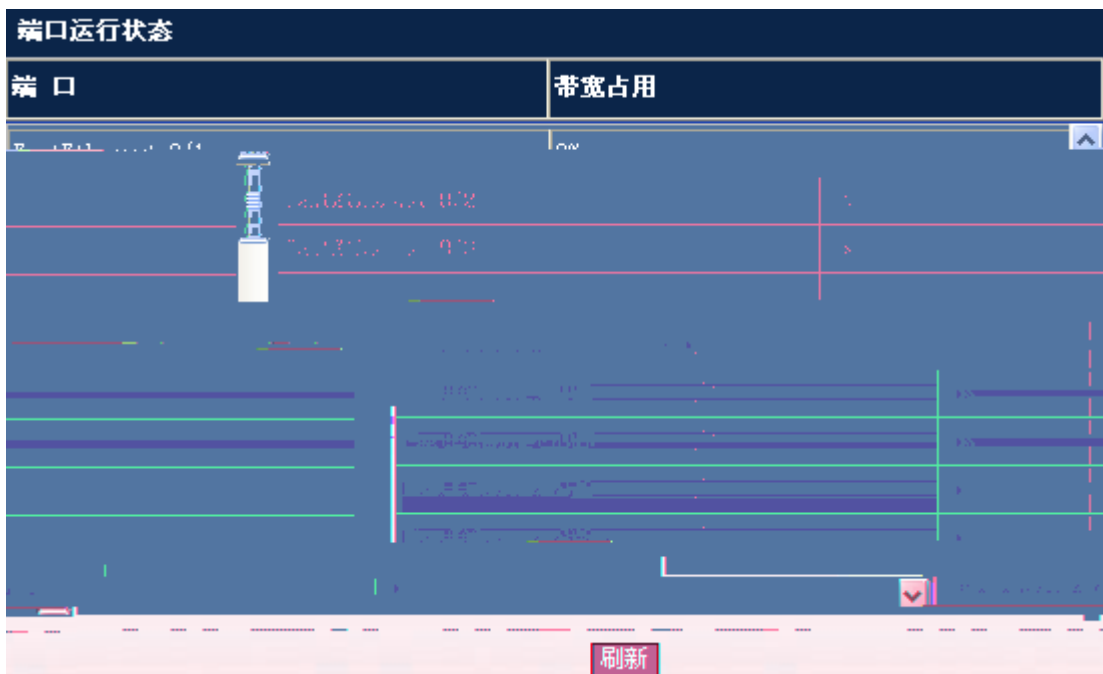
端口	描述	速率	类型	速度	状态	带宽
Unknown	Unknown	copper	↑	FastEthernet 0/1	down	1
Unknown	Unknown	copper		FastEthernet 0/2	down	2
Full	100M	copper		FastEthernet 0/3	up	1
Unknown	Unknown	copper		FastEthernet 0/4	down	900
down	Unknown	copper		FastEthernet 0/5	down	1
down	Unknown	copper		FastEthernet 0/6	down	1
down	Unknown	copper		FastEthernet 0/7	down	1
down	Unknown	copper		FastEthernet 0/8	down	1
down	Unknown	copper		FastEthernet 0/9	down	1
down	Unknown	copper	↓	FastEthernet 0/10	down	1

刷新

1.8.4

“ ”

1-82



1.8.5

“ ”

1-83

端口统计信息

注意：选择 All Ports 时，将统计所有接口的统计信息清零。选择 All Ports 时，将统计所有接口的统计信息清零。

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
14013	12012	343	1658	Gi0/1	33198	8950	5508	18740
0				Gi0/2	0	0	0	0
2717				Gi0/3	2157	2146	6	543
0				Gi0/4	0	0	0	0
175				Gi0/5	34	23	11	27
0				Gi0/6	0	0	0	0
2298818				Gi0/7	882792	404167	69848	695541
0				Gi0/8	0	0	0	0
842417				Gi0/9	437082	435647	37	191269
0				Gi0/10	0	0	0	0
2367132				Gi0/11	856226	850552	149	754472
0				Gi0/12	0	0	0	0
0				Gi0/13	0	0	0	0
0				Gi0/14	0	0	0	0
8386				Gi0/15	5557815	1423231	935630	213
0				Gi0/16	0	0	0	0

1.8.6

1-84

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: 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
28 06:20:49: %ARP_GUARD-4-SCAN: ARP scan was detected. *Feb 28 06:20:49: %ARP_GUARD-4-SCAN: ARP scan was detected. *Feb 28 06:33:51: %ARP_GUARD-4-SCAN: ARP scan was detected. *Feb 28 06:43:52: %ARP_GUARD-4-SCAN: ARP scan was detected. *Feb 28 06:53:54: %ARP_GUARD-4-SCAN: ARP scan was detected. *Feb 28 07:03:55: %ARP_GUARD-4-SCAN: ARP scan was detected. *Feb 28 07:13:56: %ARP_GUARD-4-SCAN: ARP scan was detected. *Feb 28 07:23:57: %ARP_GUARD-4-SCAN: ARP scan was detected. *Feb 28 07:33:58: %ARP_GUARD-4-SCAN: ARP scan was detected. *Feb 28 07:44:00: %ARP_GUARD-4-SCAN: ARP scan was detected. *Feb 28 07:44:01: %ARP_GUARD-4-SCAN: ARP scan was detected. *Feb 28 07:54:03: %ARP_GUARD-4-SCAN: ARP scan was detected. *Feb 28 08:04:04: %ARP_GUARD-4-SCAN: ARP scan was detected. *Feb 28 08:14:06: %ARP_GUARD-4-SCAN: ARP scan was detected.

```

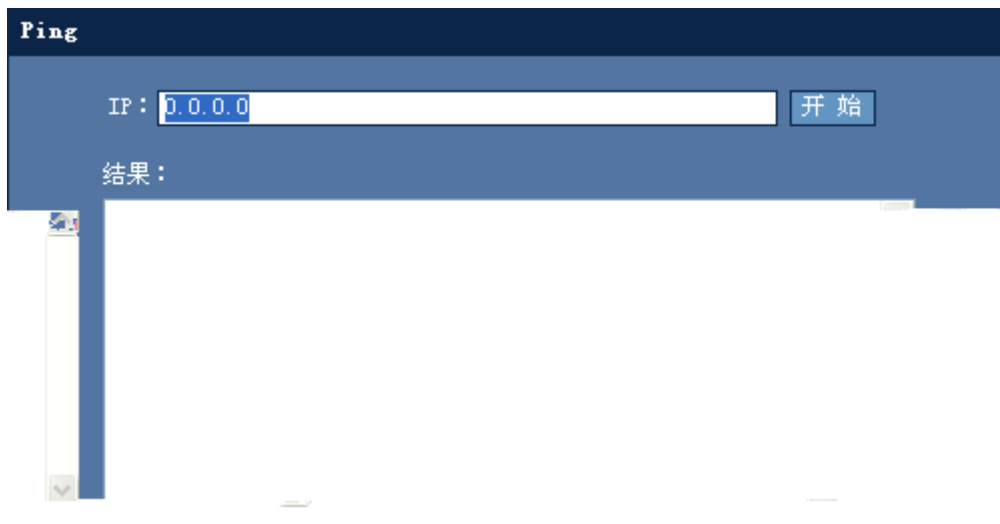
1.9

1.9.1 Ping

" Ping"

Ping

1-85 Ping



IP

" "

IP

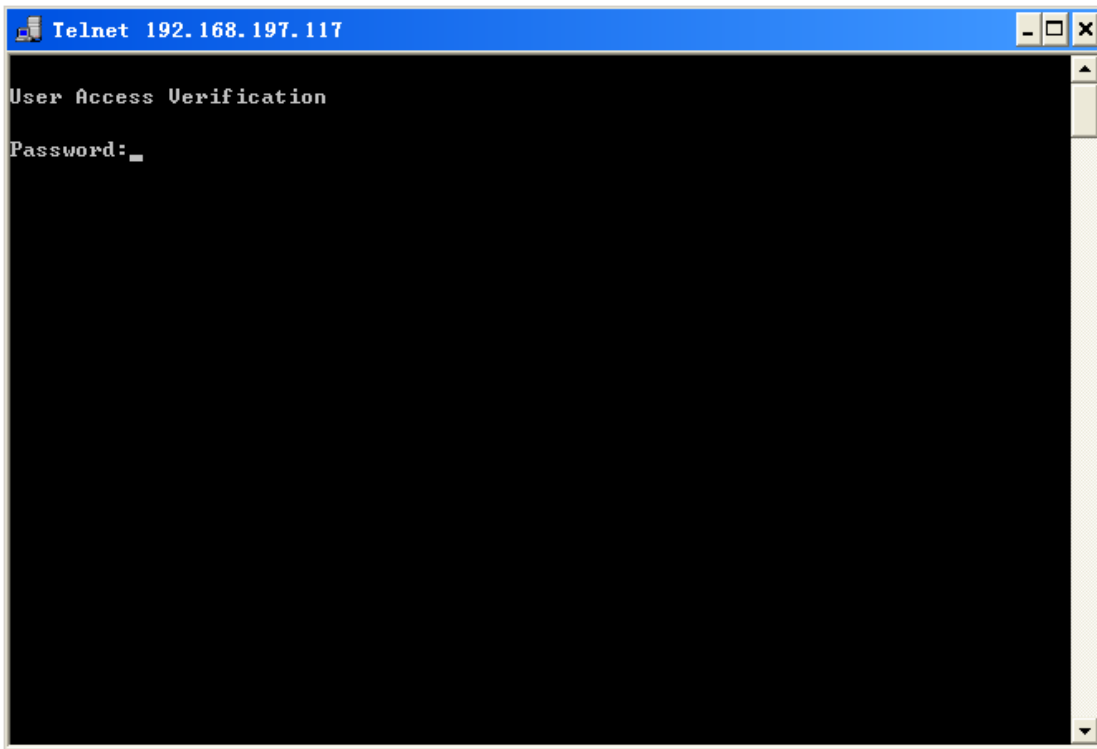
Ping

1.9.2 Telnet

" Telnet"

Telnet

1-86 Telnet



" Telnet"

Telnet

PC

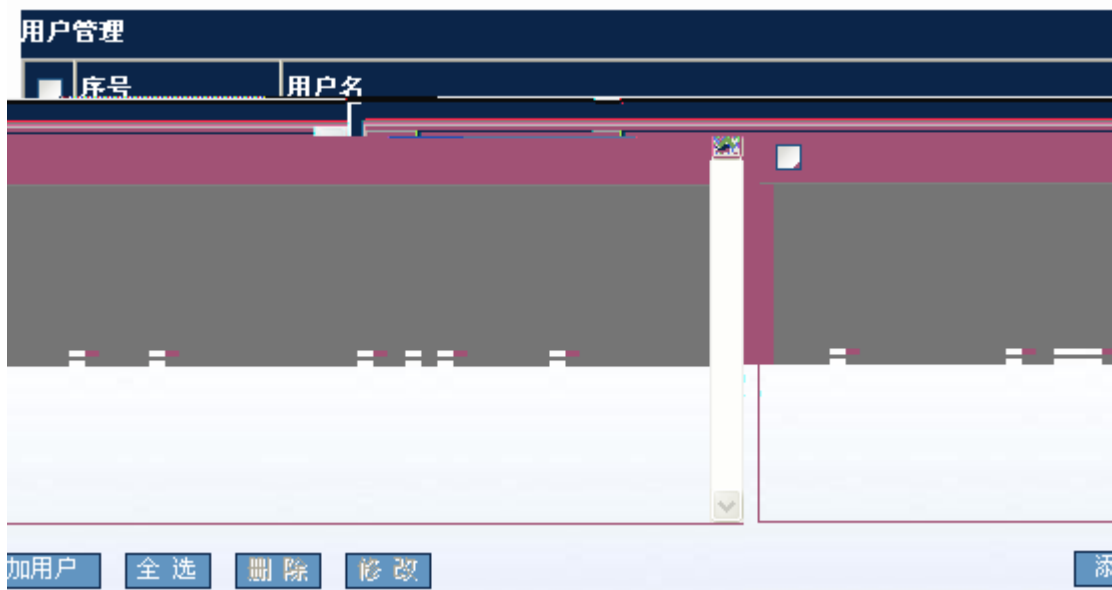
Telnet

PC Telnet

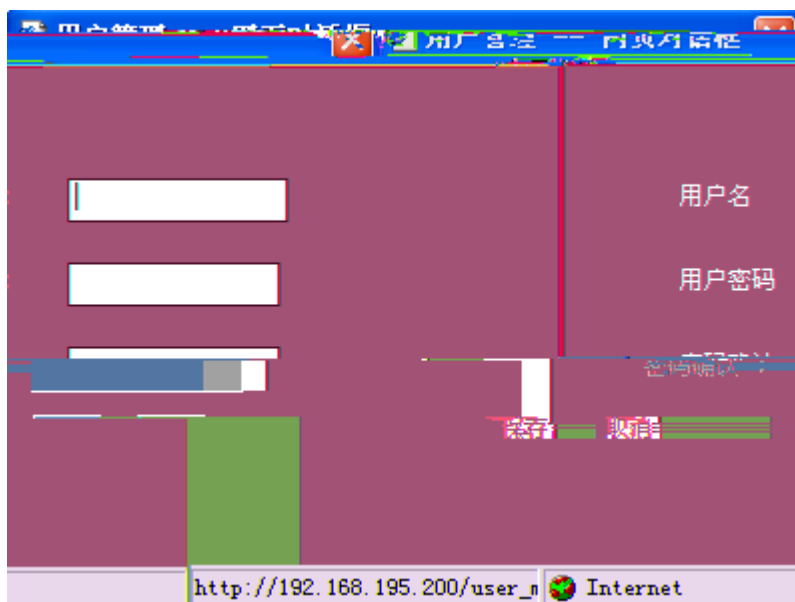
1.9.3

" "

1-87



1-88



1-89



Enable

Enable

1-91



Telnet

Telnet

1.9.5 /

" / "

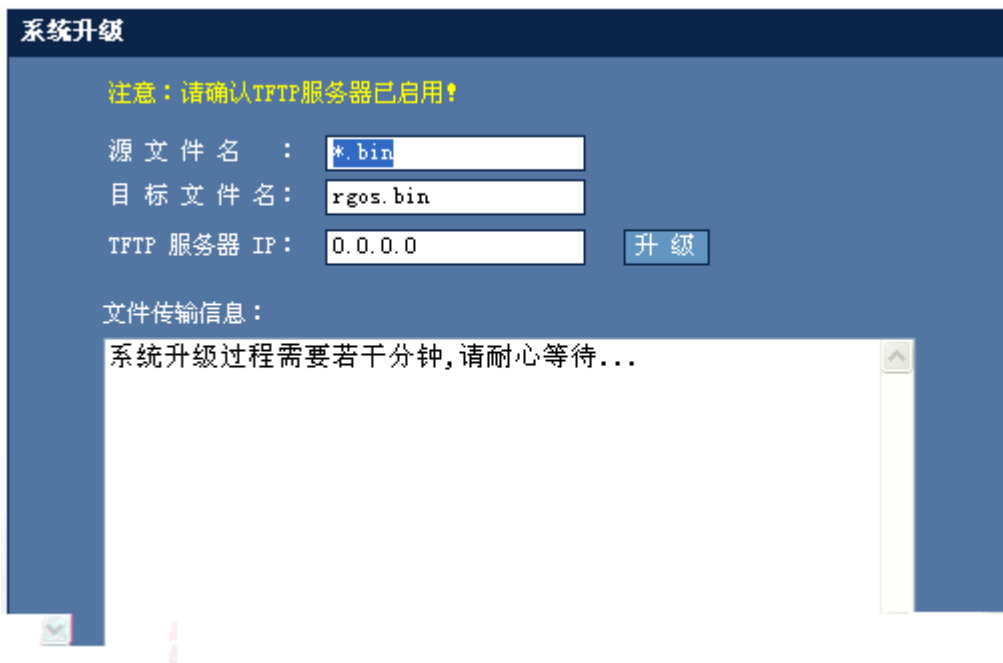
/

1-92 /

1.9.7

" "

1-94



TFTP TFTP
TFTP IP " "

1.9.8

" "

" "

1.10 WEB

WEB WEB enable

Local #) \$

```
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
```

326525

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