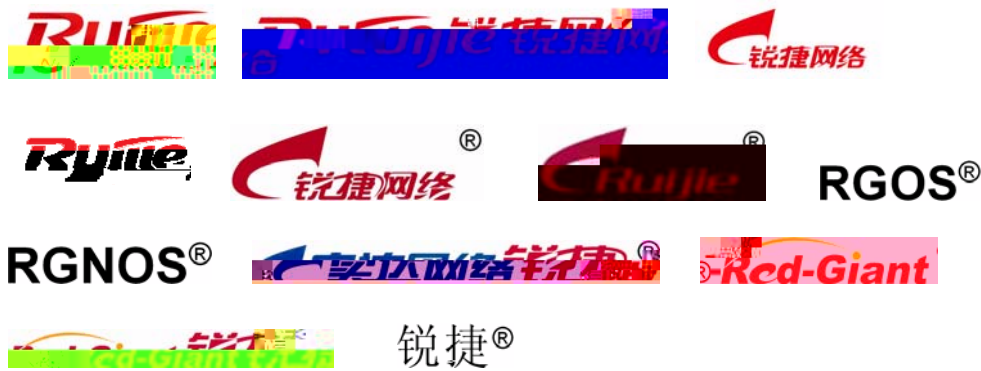




©2000-2013



■ <http://www.ruijie.com.cn/>

■ <http://webchat.ruijie.com.cn>

8:30 6

-
-
-

1.

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

2.

⚡ §
📖 §

3.

■

■

■



-WEB

南

-
1. WEB

1 WEB

1.1 WEB

WEB IE
WEB WEB WEB WEB IE
WEB WEB

1.2

1.2.1

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

1.2.2

- WEB
- WEB
- IP

1.3 WEB

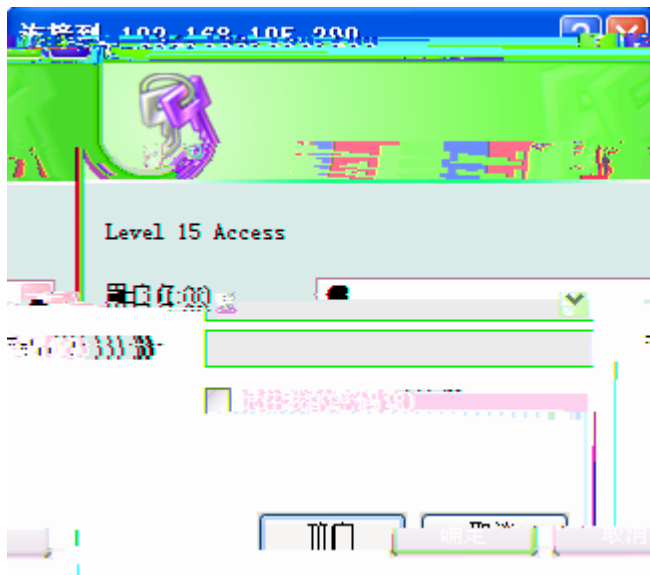
WEB WEB “ WEB ”
 WEB leBleB WEB

1-1



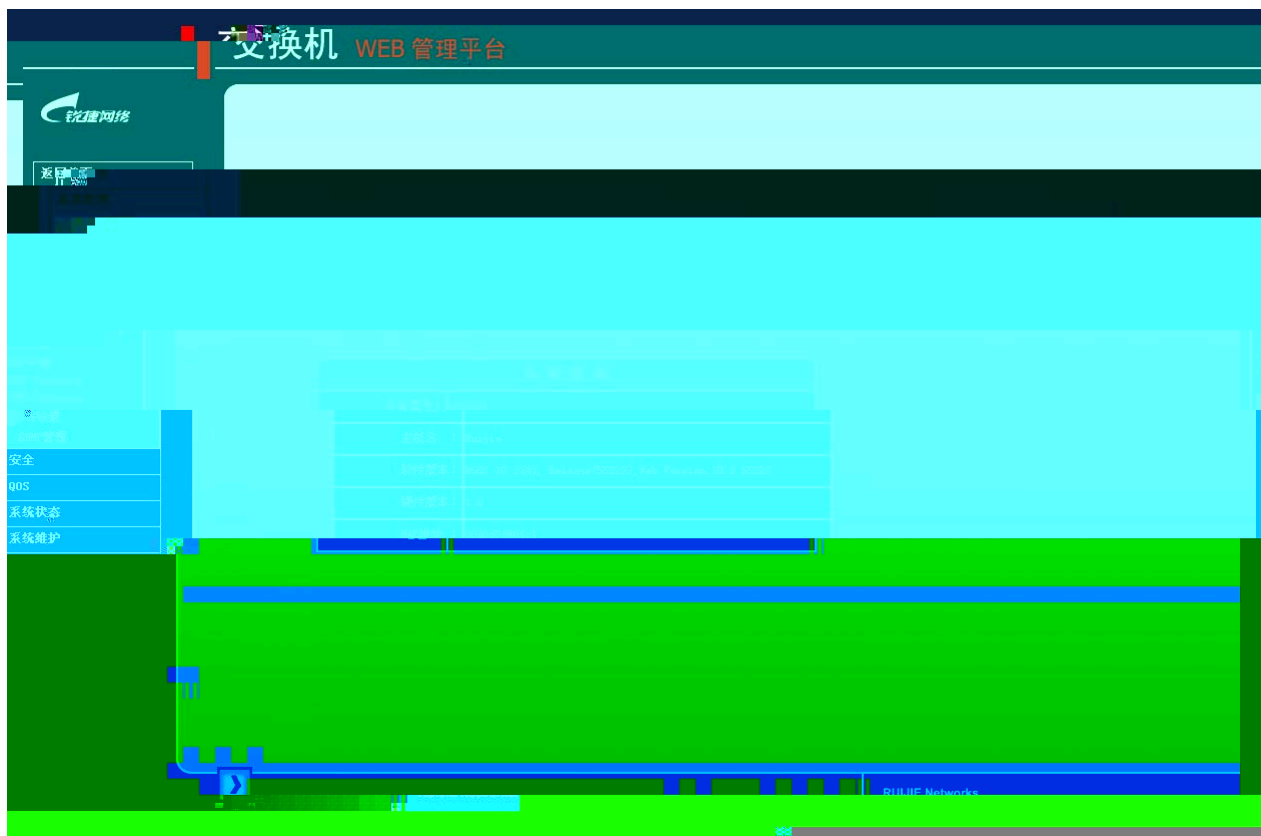
“ ”

1-2



WEB

1-3 WEB



1.5

1.5.1 IP

“ IP ”

IP

1-4 IP



VLAN

1-6 VLAN



VLAN

VLAN

VLAN

VLAN

“ ”

1-7 VLAN

VLAN管理 -- 网页对话框

VLAN ID : (1-4094)

VLAN 名称 : (可选)

保 存

取 消

VLAN ID

VLAN

“ ”

VLAN

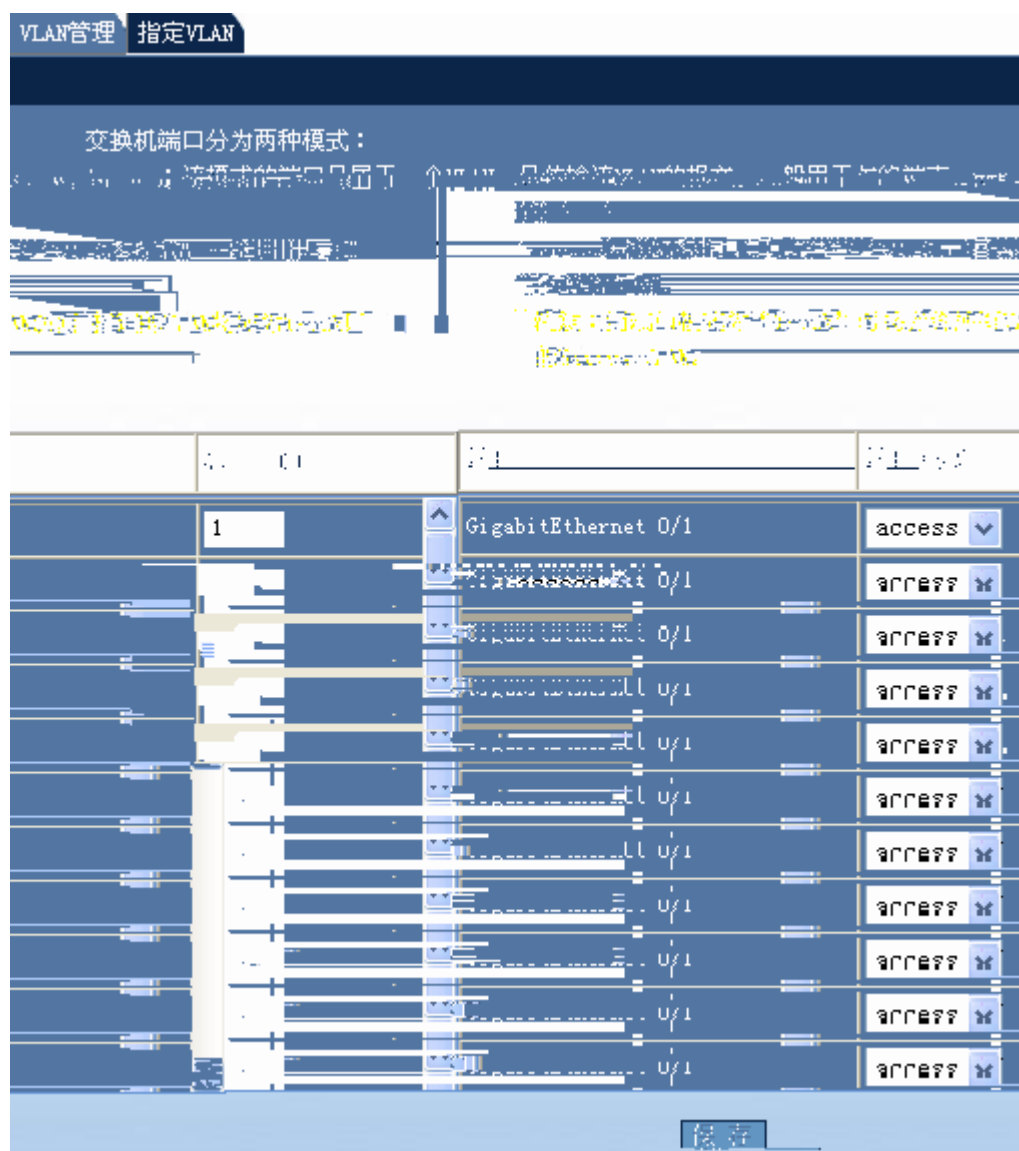
VLAN

VLAN

“ ”

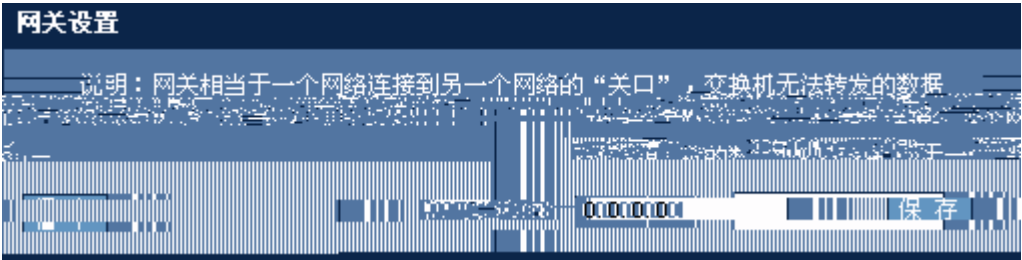
VLAN

“ ”



VLAN ID

“ ”



IP

IP “ ”

1.5.4

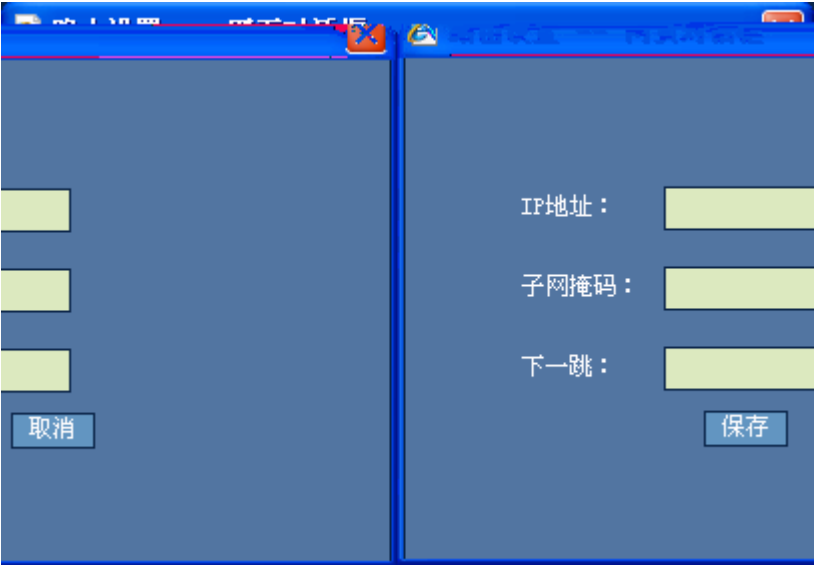
“ ”

1-11

路由设置				
☐	序号	IP地址	子网掩码	下一跳
☐	1	2.2.2.0	255.255.255.0	1.1.1.1
☐	2	192.168.23.240	255.255.255.240	192.168.23.1
添加路由 全选 删除				

“ ”

1-12



IP “ ”
“ ”

1.5.5

“ ”

1-13



1.5.6



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		
GigabitEthernet 0/2		
GigabitEthernet 0/3		
GigabitEthernet 0/4		
GigabitEthernet 0/5		
GigabitEthernet 0/6		
GigabitEthernet 0/7		
GigabitEthernet 0/8		
GigabitEthernet 0/9		
GigabitEthernet 0/10		
GigabitEthernet 0/11		
GigabitEthernet 0/12		

保 存

取消全部输出限速

“ ”

“ ”

1.5.7

“ ”

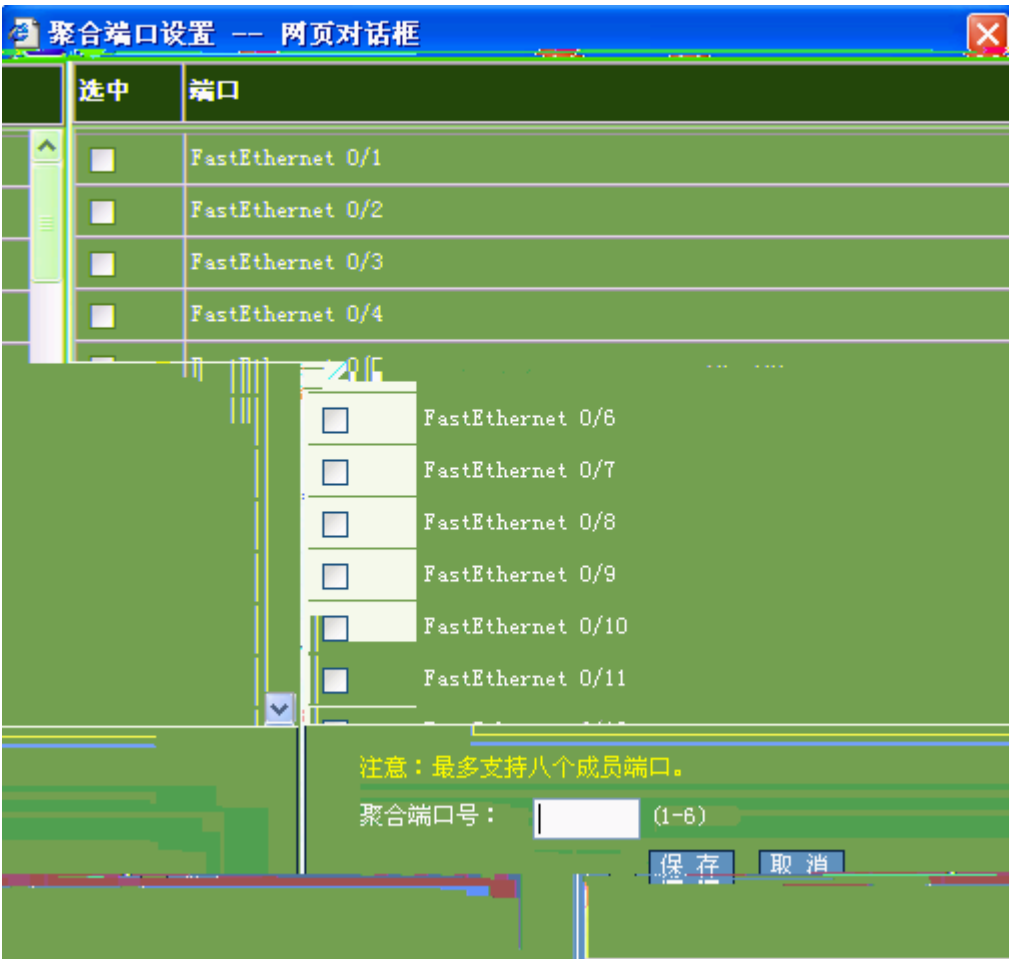


■

“ ”

■

“ ”



“ ”

■

“ ”

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	流控	描述
G10/1	Down	Half	10	On	-
G10/2	Down	Half	10	On	-
G10/3	Down	Full	1000	Off	-
G10/4	Down	Auto	Auto	Off	-
G10/5	Down	Full	100	Off	-
G10/6	Down	Auto	Auto	Off	-
G10/7	Up	Full	100	Off	-
G10/8	Down	Auto	Auto	Off	-
G10/9	Down	Full	100	Off	-
G10/10	Down	Auto	Auto	Off	-
G10/11	Down	Auto	Auto	Off	-
G10/12	Down	Auto	Auto	Off	-

“ ”

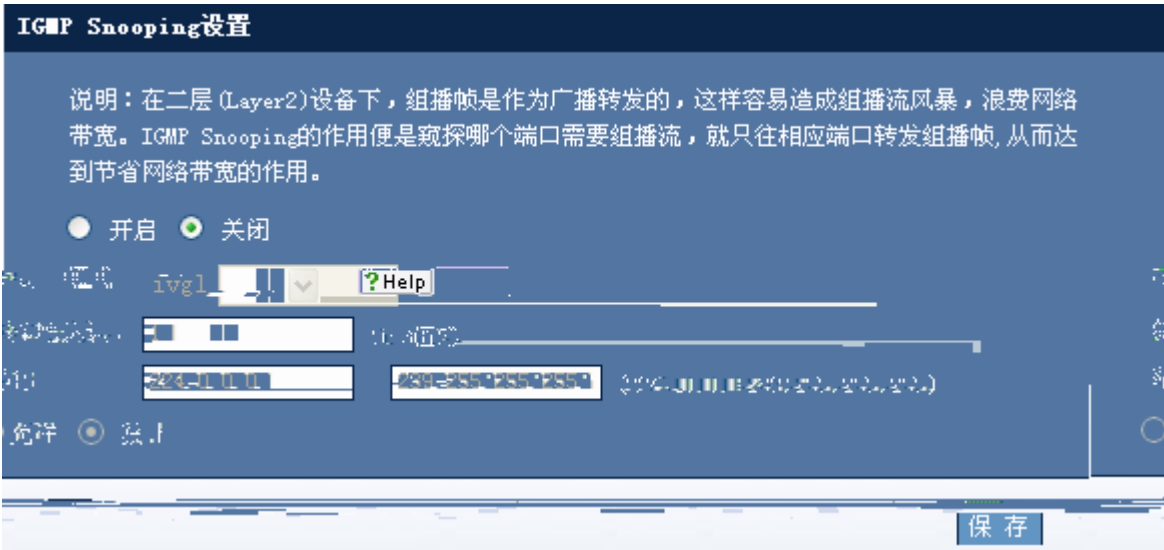
1.5.9 DHCP

“ DHCP ”

DHCP

1-19 DHCP





IGMP Snooping “ ” ivgl
svgl ivgl-svgl svgl ivgl-svgl IP “ ”
IGMP Snooping “ ” “ ”

1.5.11 STP

“ STP ”

STP

1-21 STP

STP设置

说明：STP通过有选择性地阻塞网络中的多余链路，保证网络中无环路产生；若网络出现故障导致链路失效，又能提供相应的链路备份，保证网络稳定运行。

开启STP功能：☒（默认开启的是MSTP）保存

MSTP基本设置：

MST名称：

(如输入100或100-200或100-200/250/300-2000)

保存

MST修改值： (0-65535)
实例值： (1-64)
VLAN范围：

端口设置：
端口：

☐ 设为快速端口 ☐ 开启BPDU过滤 保存

MST 实例-VLAN 对应表:		
	实例	VLAN
↑ ↓		

全选删除

“ STP ” “ ”

STP
BPDU

MSTP

“ ”

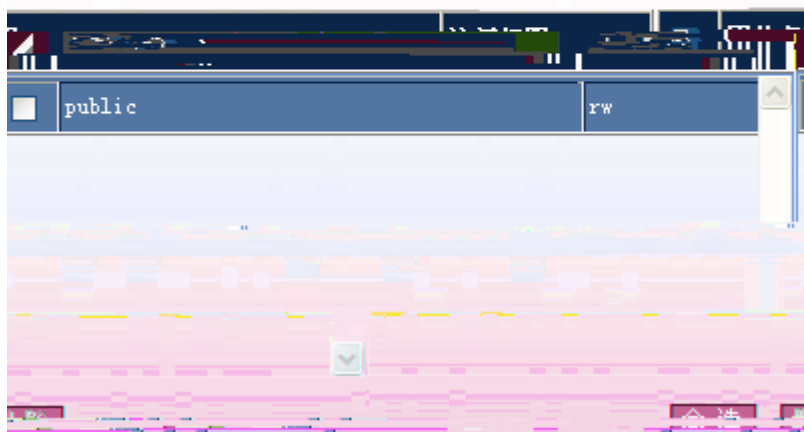
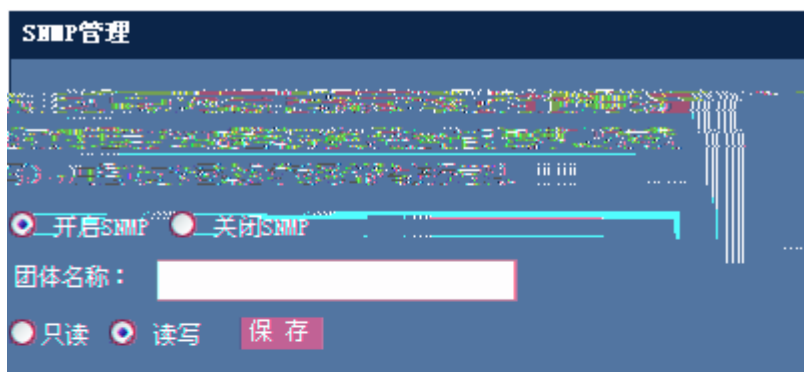
MSTP

MSTP	MSTP	VLAN
------	------	------

-VLAN -VLAN

G6-€1xP0.}3Î'° = MP |

SM? . 2 í P



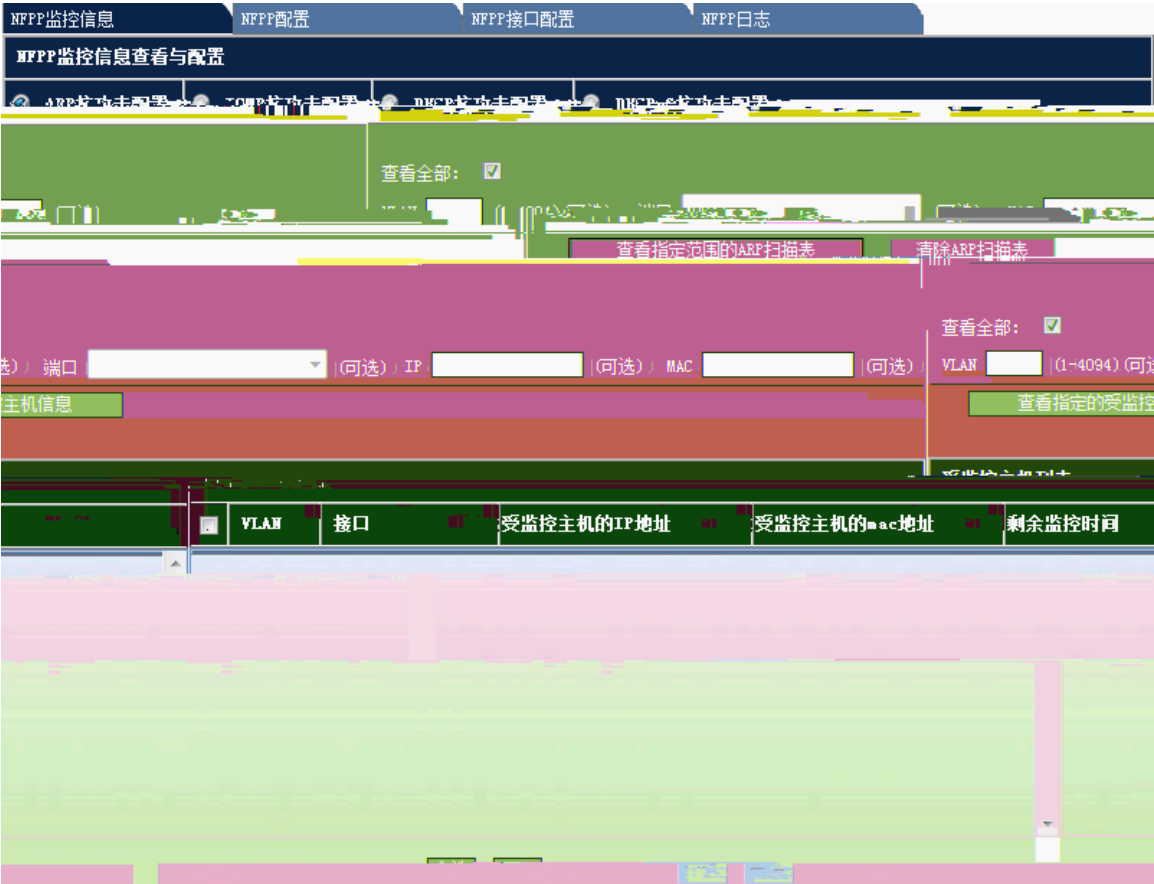
“ SNMP ”
“ ”
“ SNMP ”
“ ”

1.5.13 NFPP

“ NFPP ”

NFPP

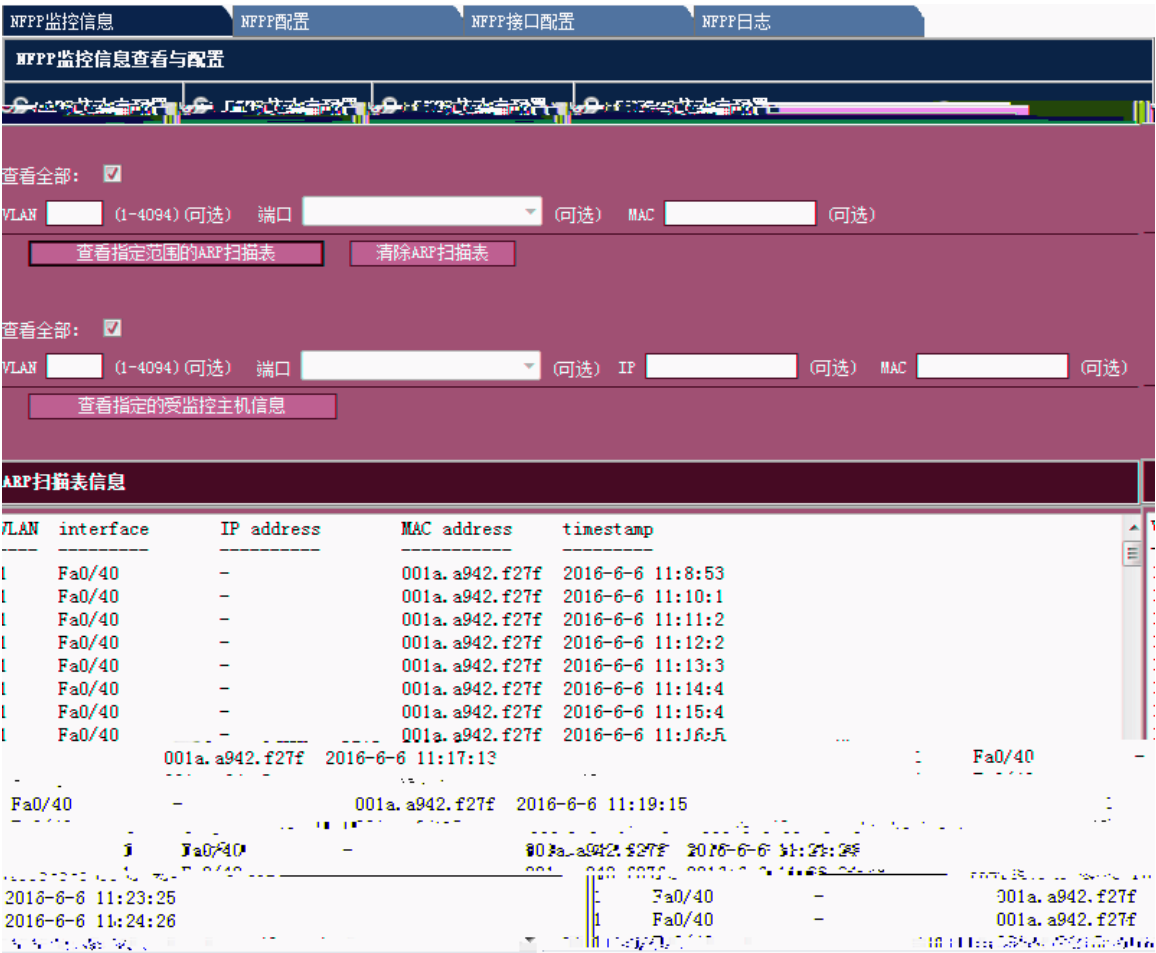
1-23 NFPP



NFPP

1) ARP

1-24 NFPP —ARP



ARP “ ARP ”

ARP “ ” ARP

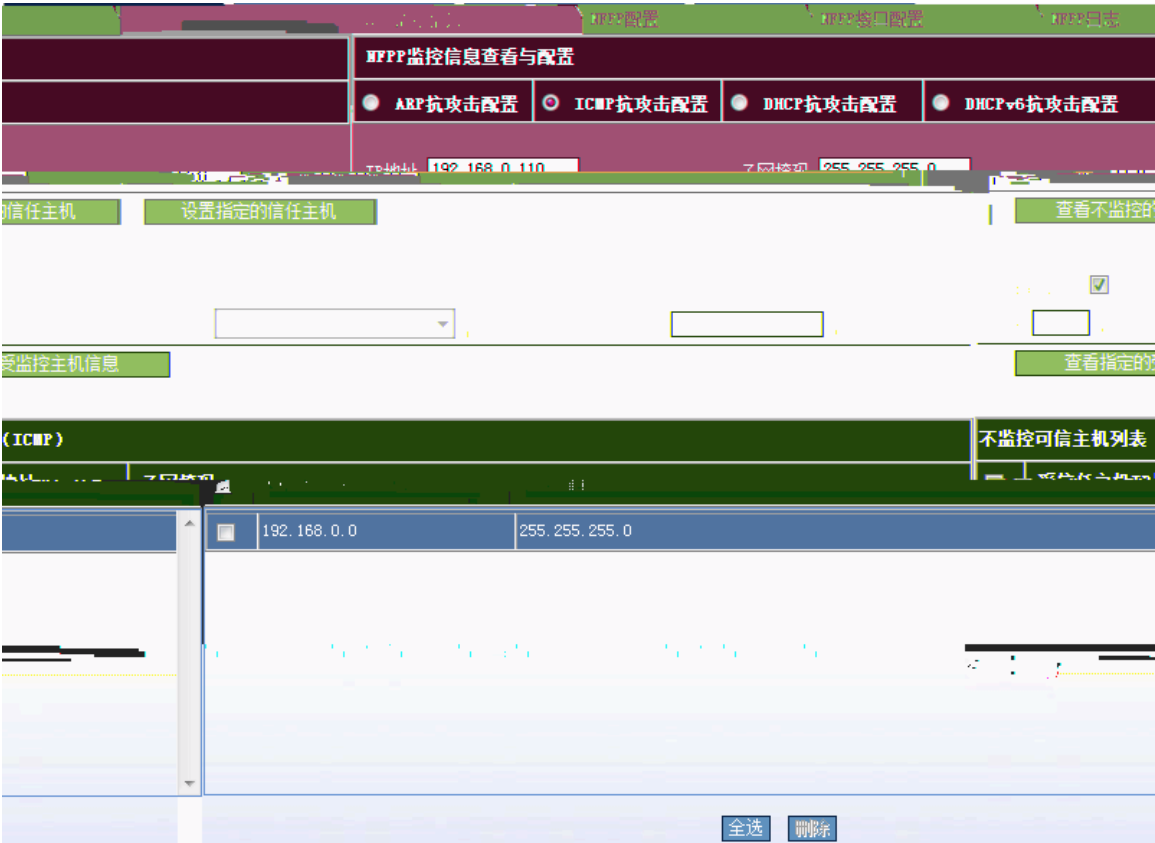
“ ARP ” ARP “ ”

“ ” “ ” “ ” “ ”

”

2) ICMP

1-25 NFPF —ICMP



ICMP “ ”

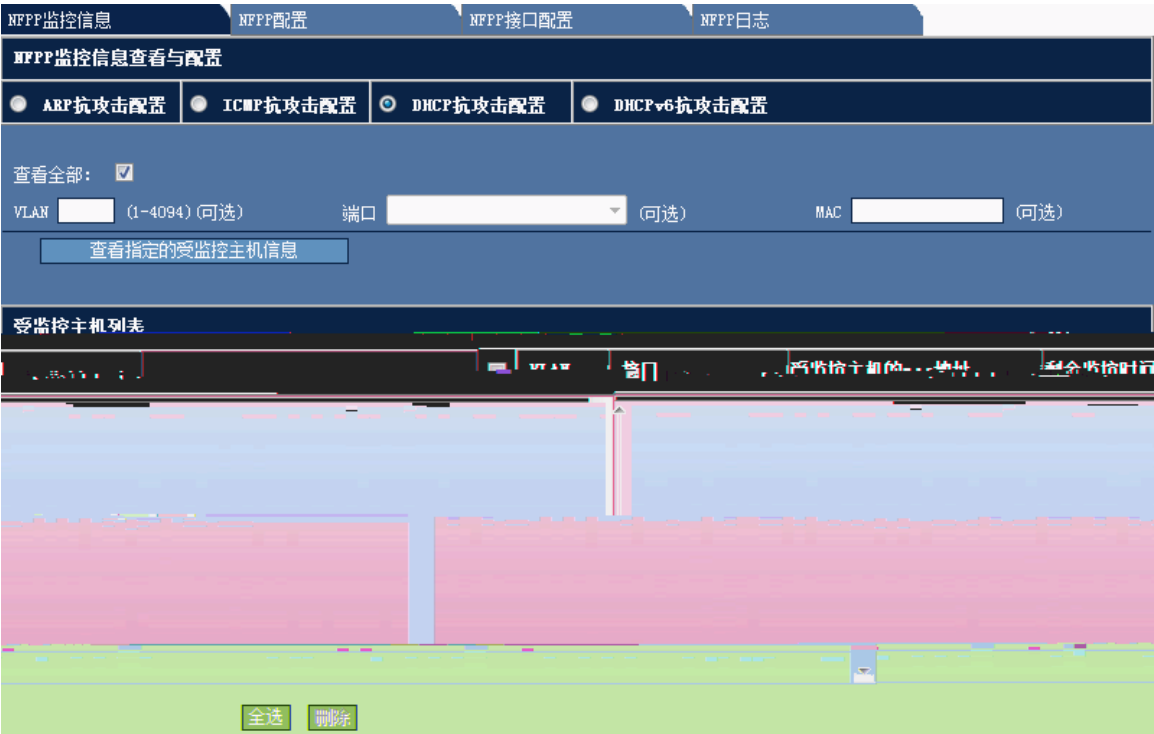
IP “ ”

“ ” “ ”

”

3) DHCP

1-26 NFPP —DHCP



DHCP “ ” “ ”

4) DHCPv6

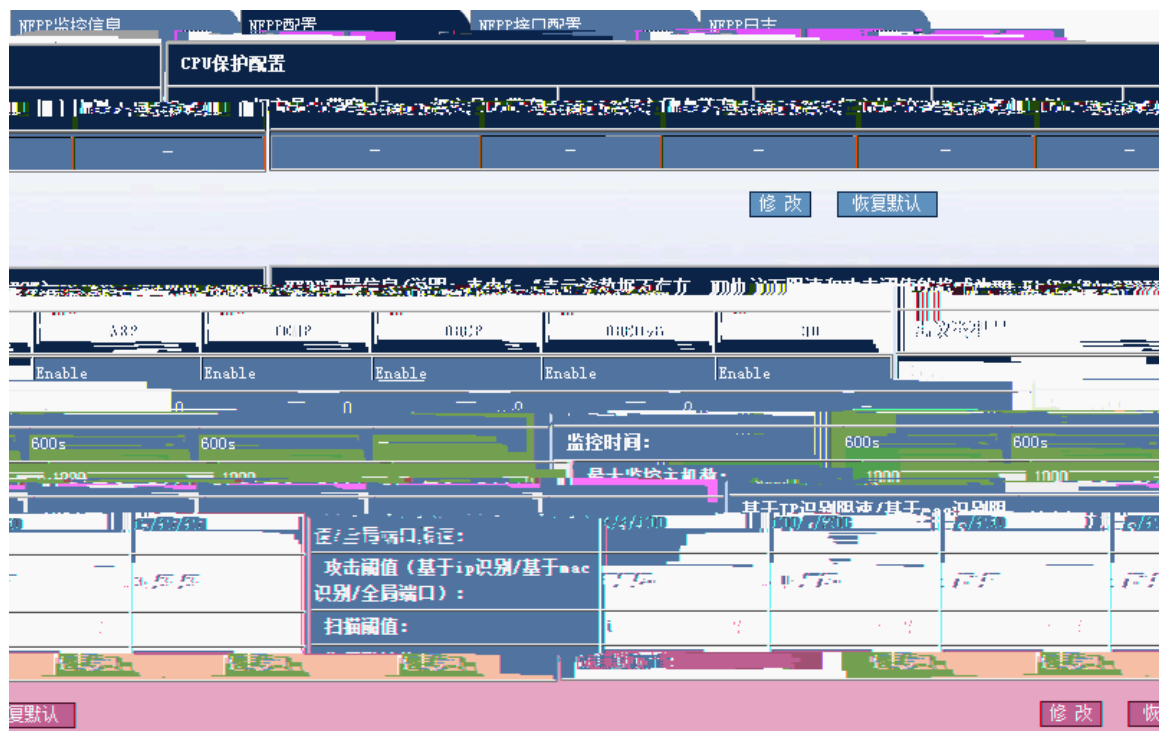
1-27 NFPP —DHCPv6



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

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

DDoS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/vi d/端口识别主机

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

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

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		接口	ARP 攻击
	123	123/789/123	123/789/456	123		Fa0/1	Enable

全选

删除

配置

默认

接口: FastEthernet 0/1

☐ 开启ICMP抗攻击

☒ 关闭ICMP抗攻击

(1-9999)

基于ip/mac/端口识别主机 (可选):

限速值: 1112 (1-9999)

攻击阈值: 1222

(1-9999)

基于port端口识别主机 (可选):

限速值: 1322 (1-9999)

攻击阈值: 2222

隔离时间: Permanent (0/30-86400) (可选)

☒ 永久隔离

保存

于IP/MAC/PORT	接口	ICMP抗攻击状态	隔离时间	限速值 (基于IP/MAC/PORT)	攻击阈值 (基
	Fe0/1	Enable	Permanent	1112/-/1322	1222/-/2222

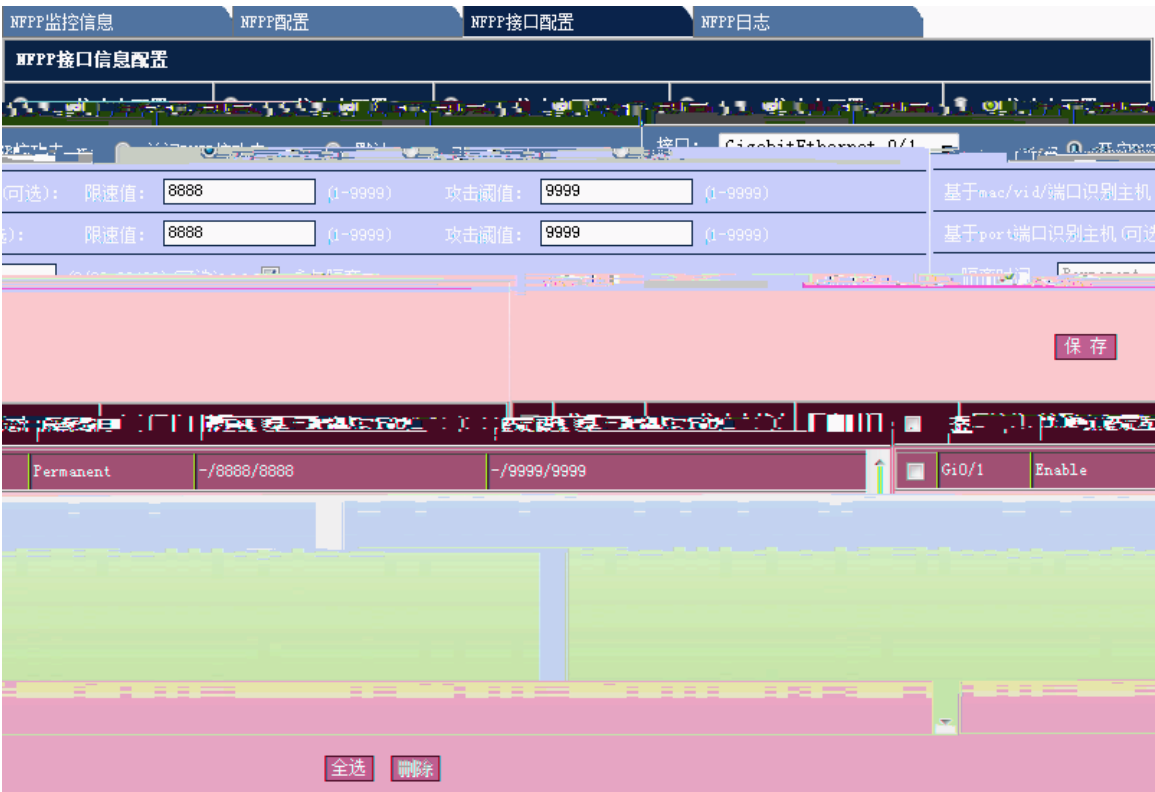
全选

删除

ICMP NFPP “ ”

3) DHCP

1-33 NFPP —NFPP DHCP



DHCP NFPP “ ”

4) DHCPv6

1-34 NFPP —NFPP DHCPv6

NFPP监控信息

NFPP配置

NFPP接口配置

NFPP日志

攻击配置

ND攻击配置

攻击

默认

9999

(1-9999)

9999

(1-9999)

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抗攻击

关闭DHCPv6抗攻击

基于mac/vid/端口识别主机(可选):

限速值: 8888

(1-9999)

攻击阈值:

基于port端口识别主机(可选):

限速值: 8888

(1-9999)

攻击阈值:

隔离时间: Permanent

(0/30-86400)(可选)

永久隔离

保存

MAC(PORT)	接口	DHCPv6抗攻击状态	隔离时间	限速值(基于IP/MAC/PORT)	攻击阈值(基于IP/MAC/PORT)
	☐ Gi0/1	Enable	Permanent	-/8888/8888	-/9999/9999

全选

删除

DHCPv6 NFPP “ ”

5) ND

1-35 NFPP —NFPP ND



ND NFPP “ ”

NFPP

1-36 NFPP



NFPP

“ ”
“ ”
“ ”

1.6

1.6.1 ARP

“ ARP ”

ARP

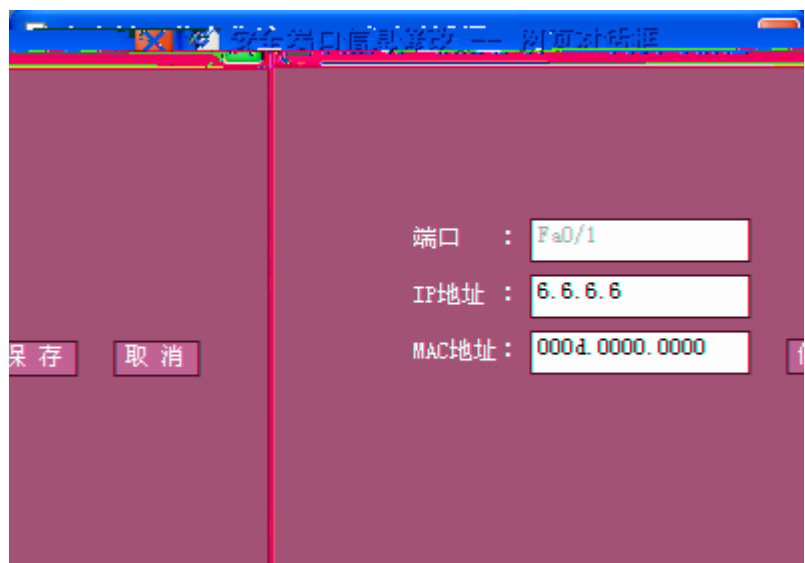
1-38 ARP





“ ”

1-40



“ ”

1.6.3 APR

“ ARP ”

ARP

1-41 ARP

“ ARP ”

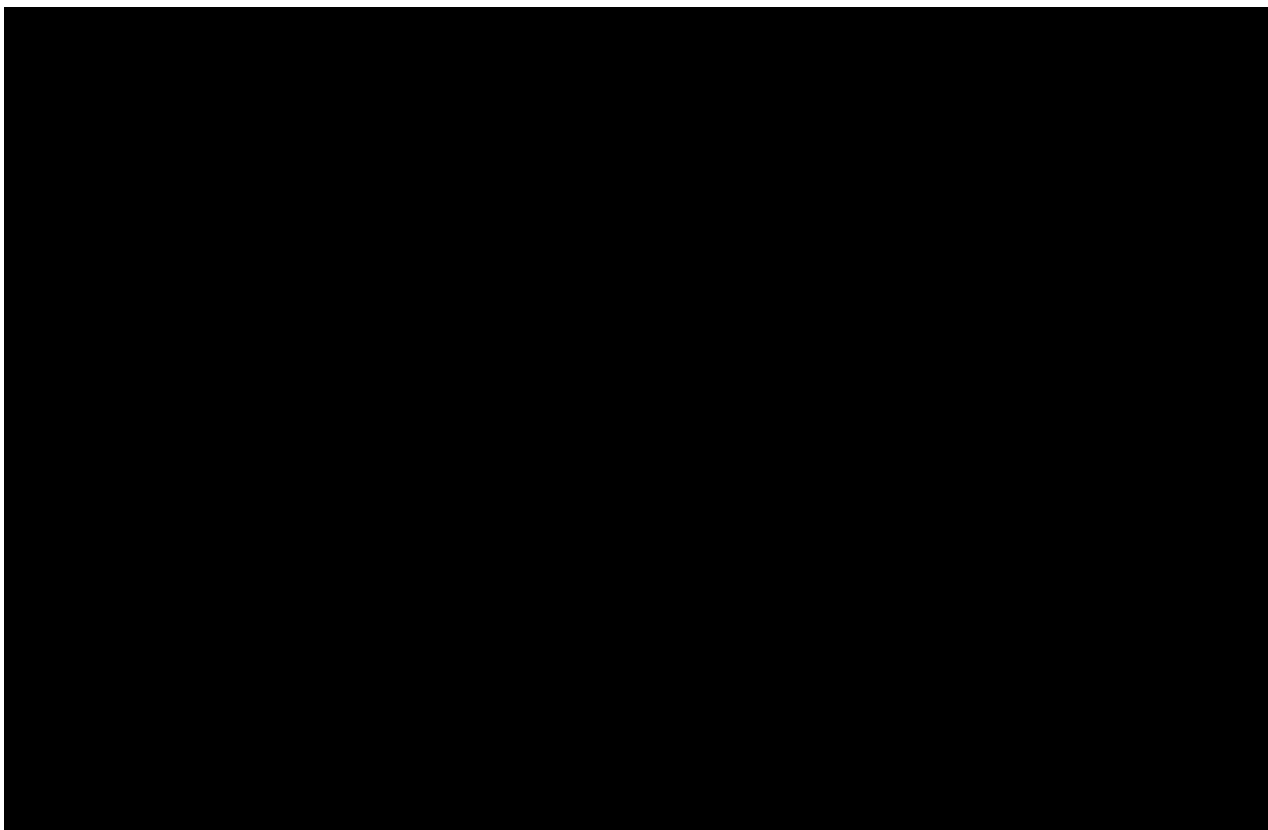
“ ARP ”

1.6.4 ACL

“ ACL ”

ACL

1-42 ACL



ACL

ACL

ACL

ACL

ACL \$ & /\$ & /

“ ” “ ”

ID

IP IP , IP “ ”

IP “ IP ” IP

1-44 IP

“ ” “ ”

ID

TCP UDP IP ICMP

IP IP IP

IP IP IP

“ ”

ACL

1-45 ACL



ACL	ACL			
	“	”		
			“	”
a	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

接口配置

用户绑定

打开接口上的IP Source Guard功能

IP Source Guard功能的应用是和DHCP Snooping结合起来的，也就是说基于接口的IP Source Guard仅仅在DHCP Snooping控制范围内的非信任口上生效，在其他信任口或者非DHCP Snooping控制范围内的接口上配置该功能，功能将不会生效。

说明：IP Source Guard功能仅在DHCP Snooping控制范围内的接口上生效，功能将不会在其他接口上生效。

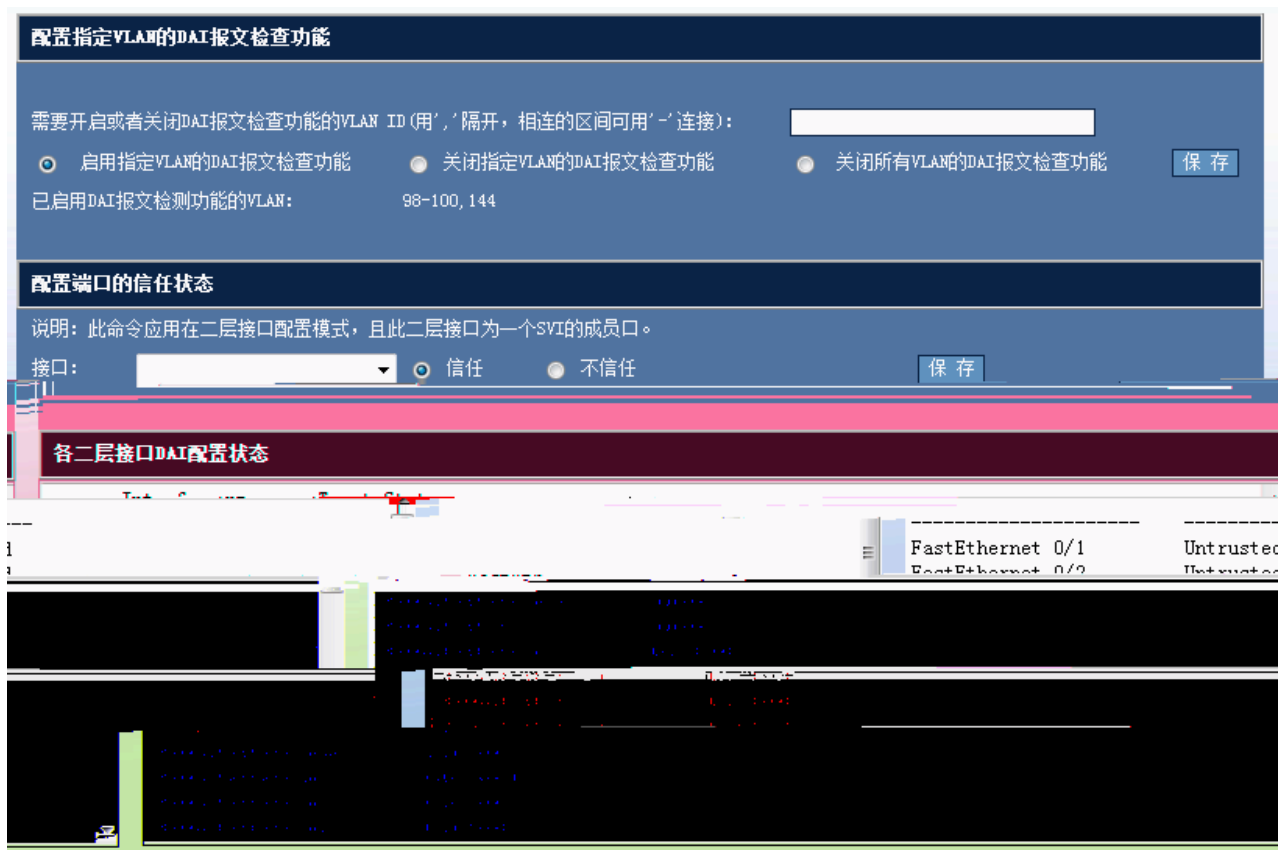
查看指定端口

查看全部

☐	接口	过滤类型	过滤模式	IP地址	MAC地址	VLAN
☐	FastEthernet 0/6	ip	active	deny-all	-	-
☐	FastEthernet 0/14	ip	active	deny-all	-	-

全选

删除



■ VLAN DAI

VLAN DAI

GSN “ ”

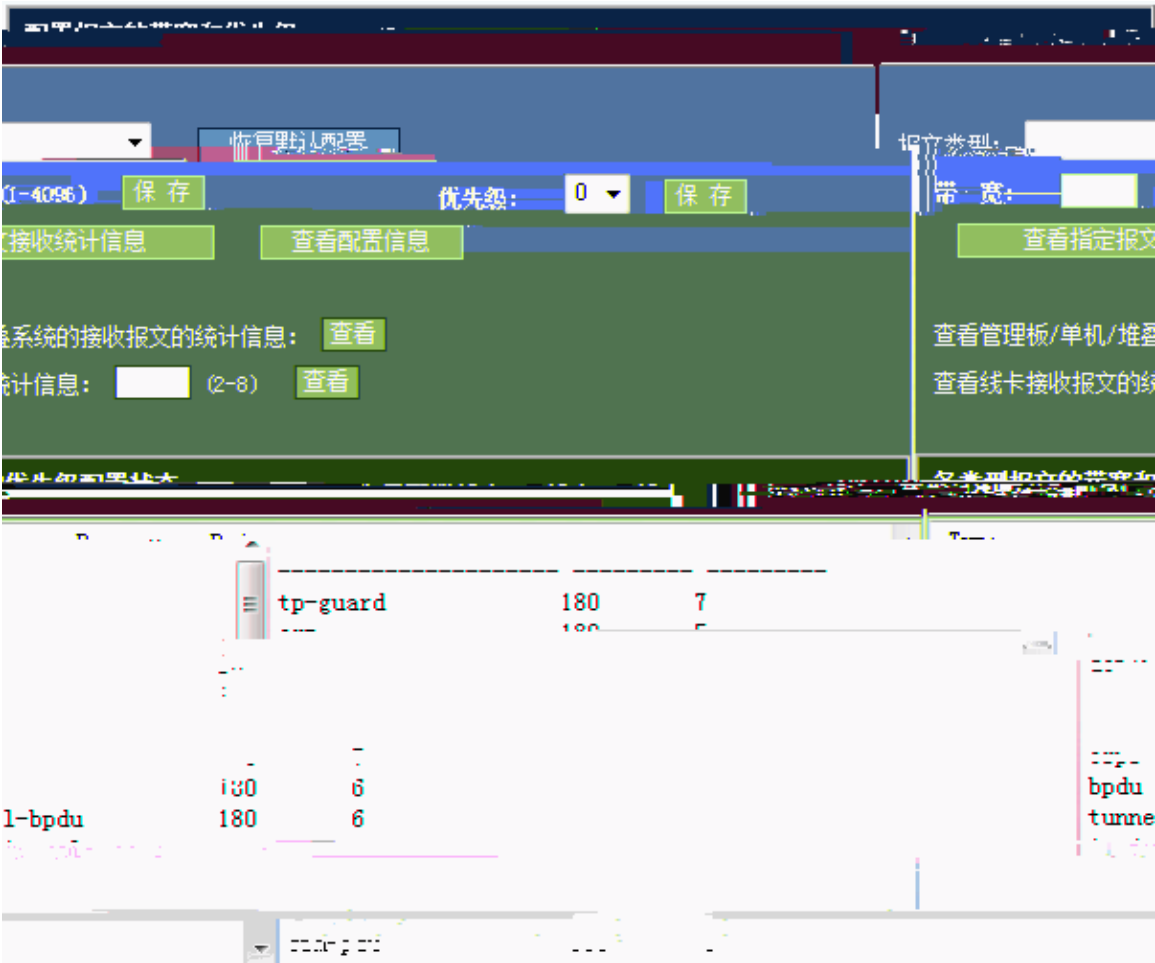
“ ”

1.6.8 CPP

“ CPP ”

CPP

1-50 CPP



“ ”

“ ”

“ ”

1-51

“ ”

1-52

各类型报文的带宽和优先级配置状态			
Type	Bandwidth	Priority	
ip-guard	180	7	
dot1x	2000	4	
rldp	180	7	
	180	7	rerp
	180	7	erps
	180	7	hndu
tunnel-bpdu	180	6	
ipv4-icmp-local	1600	6	
lldp	180	5	
lldp_cdp	180	5	
cfn-pdu	180	3	

/ / “ ” / /

1-53 / /

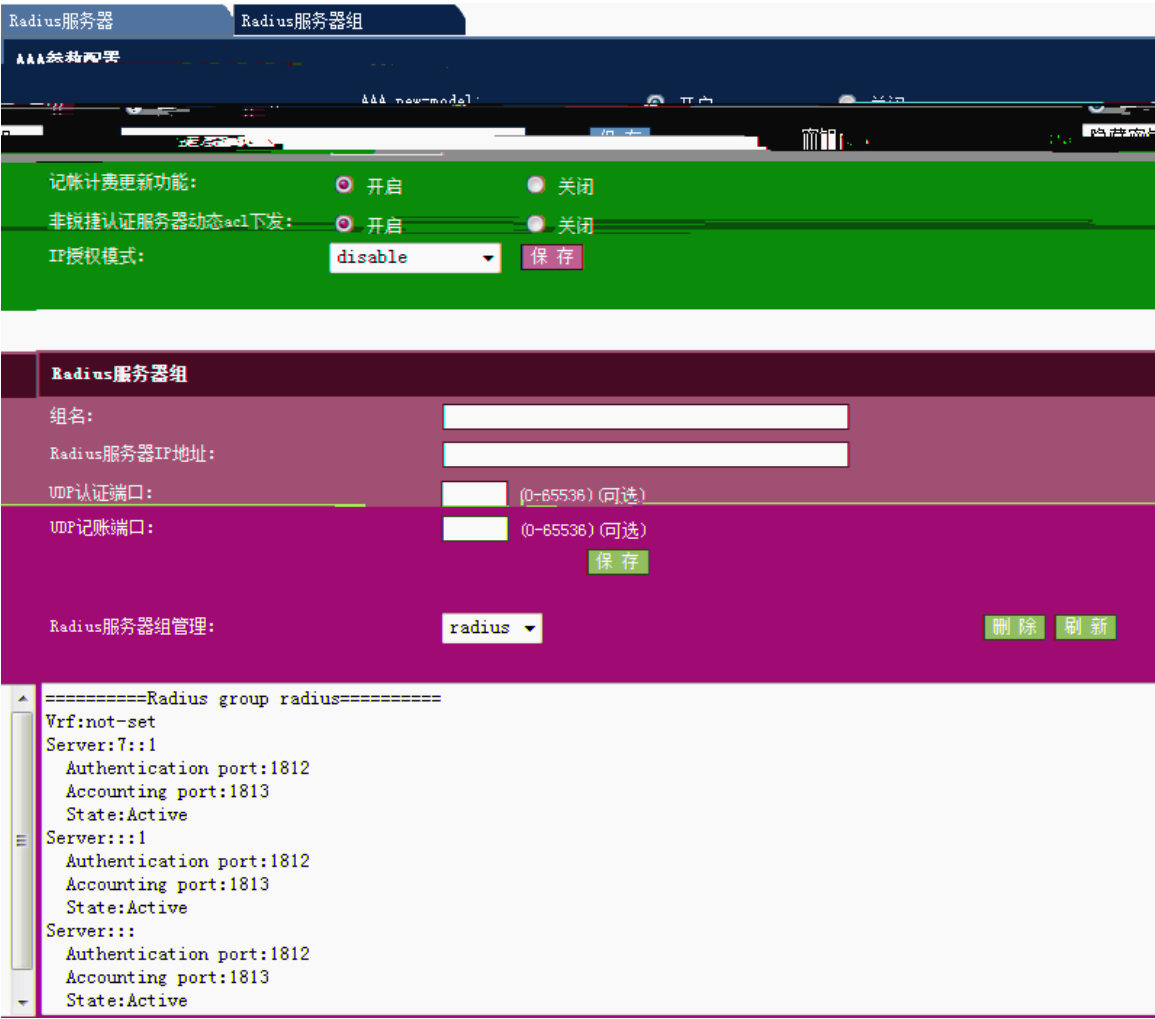
“ ”

1.6.9 RADIUS

“ RADIUS ”

RADIUS

1-54 RADIUS



“ ”

Radius

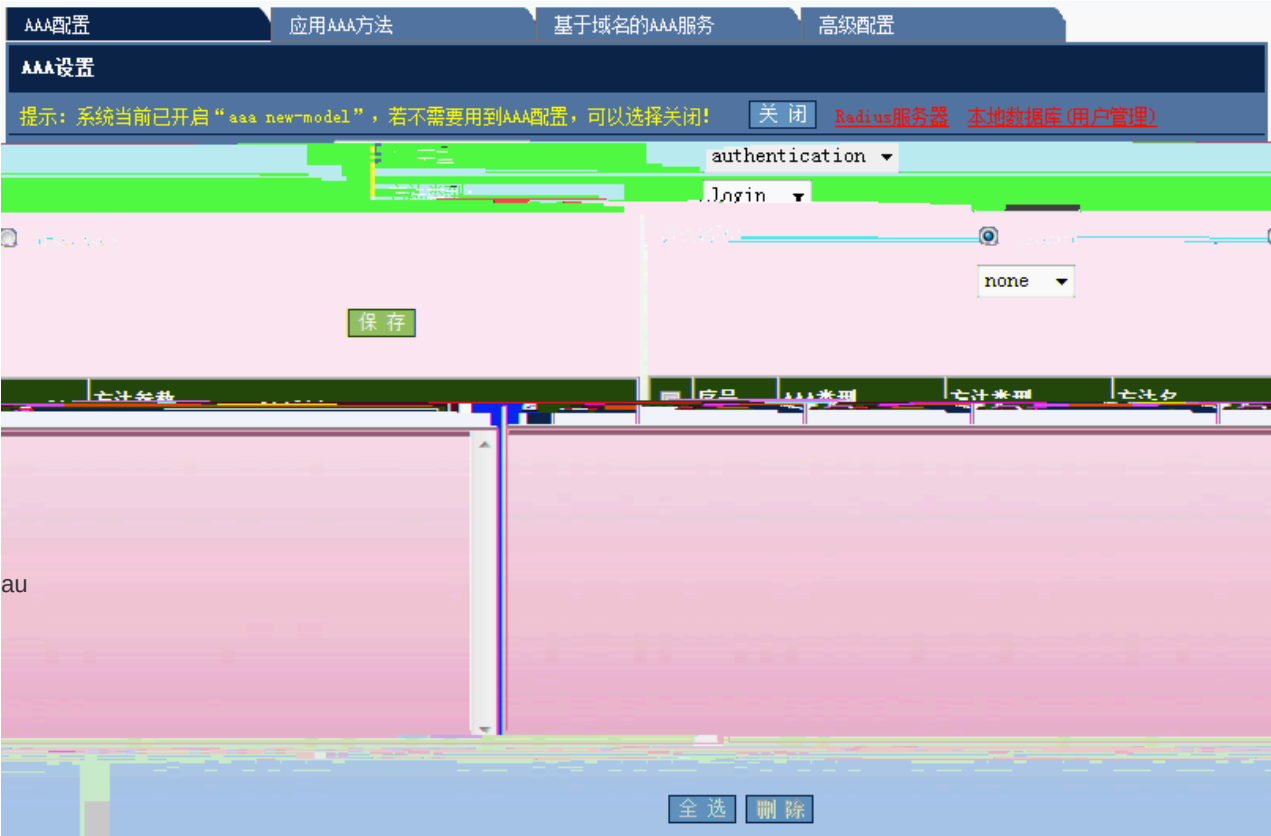
“ ”

1.6.10 AAA

“ AAA ”

AAA

1-56 AA A

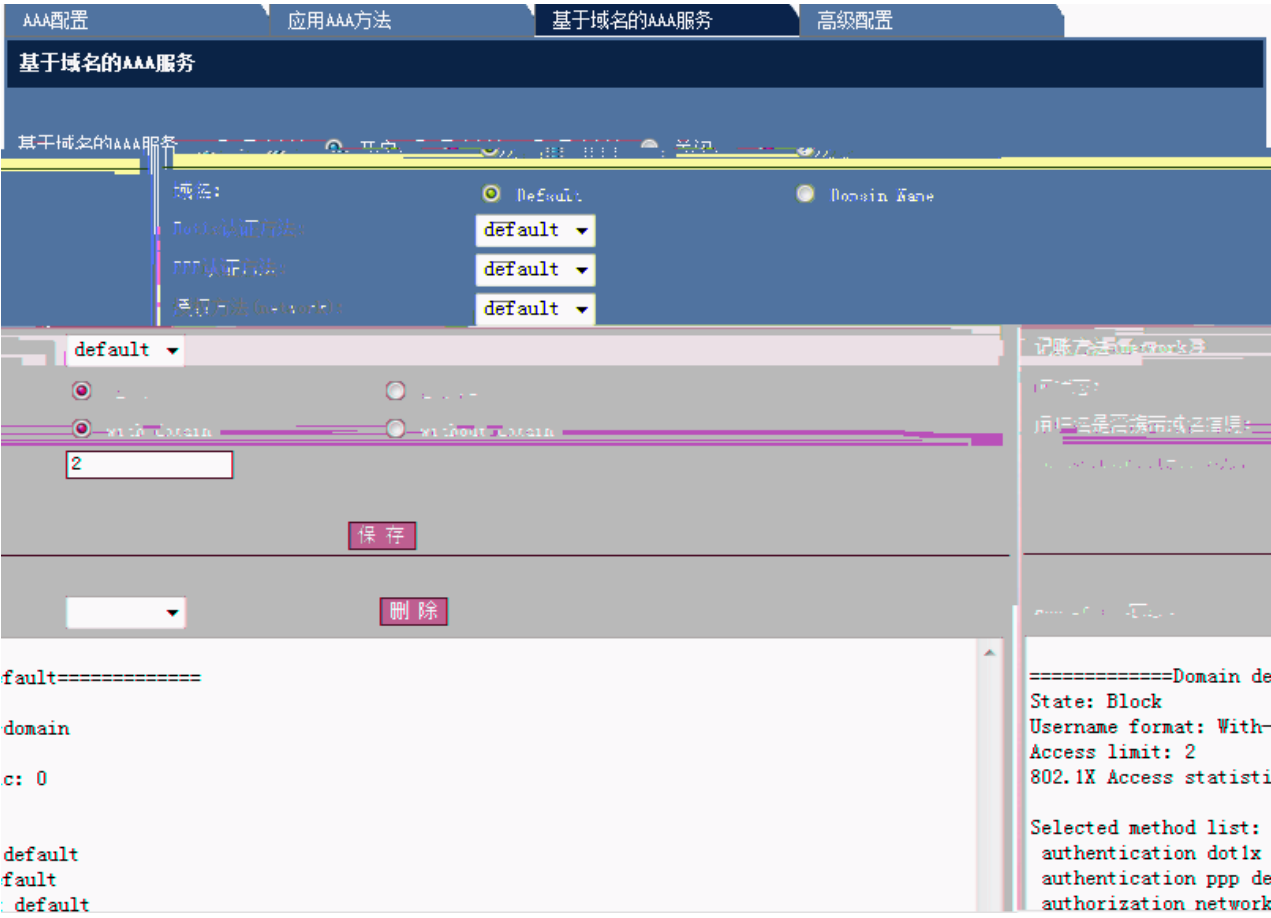


AAA

AAA	authentication authorization accounting	AAA	login enable
en	È \$ #ø©2O r\$ðÕñàÑ"r\$ðÝÐ Ý ½		

AAA

1-58 AAA

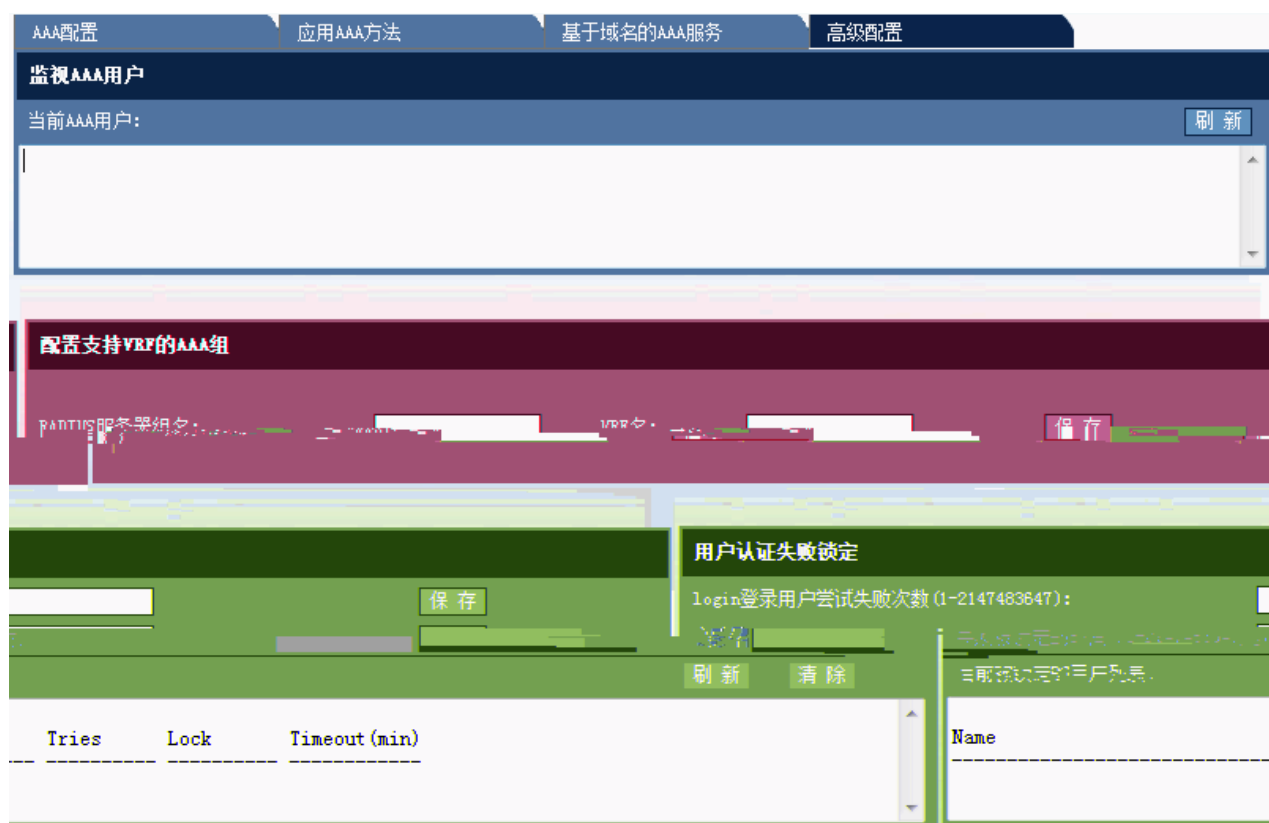


AAA Dot1x PPP (network) (network)

Access Limit “ ” \$

AAA Domain “ ”

1-59 AA A



AAA

AAA

VRF AAA

1.6.11 Dot1x

“

Dot1x

“ ” “ ”

1-61

、 11κ “ ” “ ” Ø * Ω

Dot1x配置

主动认证配置

端口认证配置

说明：以下配置项均为可选。

端口：

FastEthernet 0/1

802.1x认证功能：

开启

关闭

VLAN自动跳转功能：

开启

关闭

Guest Vlan跳转：

开启

关闭

Vlan Id： (1-4094)

端口的控制模式：

基于用户MAC

基于端口单用户的控制模式

MAC旁路认证：

开启

关闭

MAC旁路认证超时时间： (1-65535)

MAC旁路认证违例：

开启

关闭

保存

恢复默认

查看当前配置

禁止动态用户在多个认证端口之间迁移：

开启

关闭(默认值)

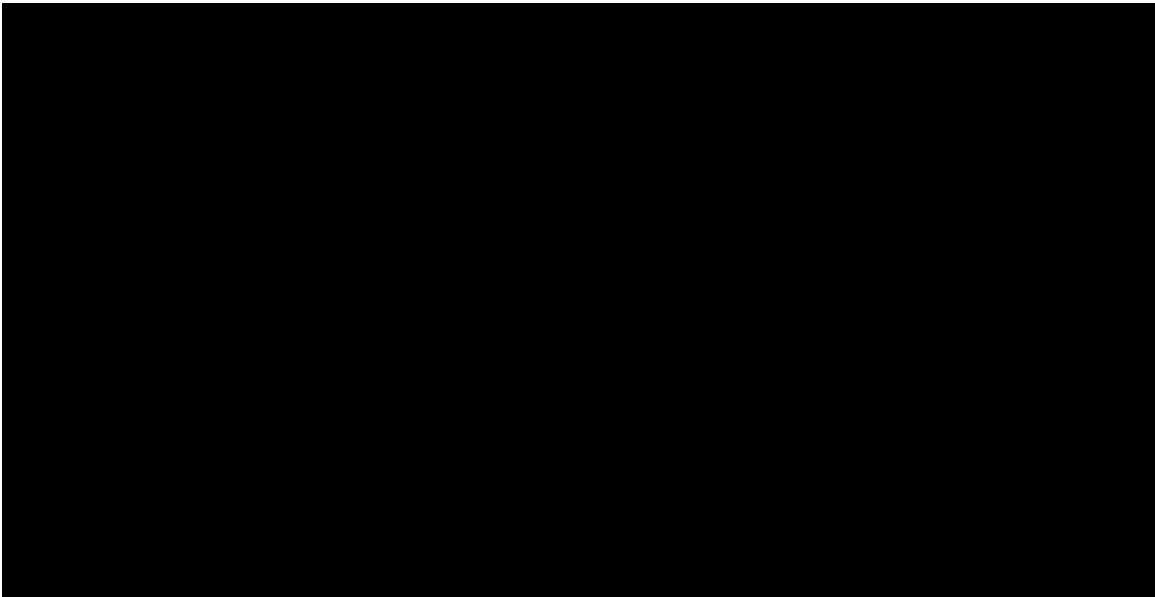
保存

端口下可认证主机列表

主机IP地址

端口

Dot1x



“ ”

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

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

1.6.13 WEB

“web”

web

1-66 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

重定向的IP地址:

0.0.0.0

认证页面URL:

重定向端口 (最多可以配置10个，中间使用英文逗号分开):

80

未认证用户的最大HTTP会话数 (0-255，可选):

255

每个端口下 (1-85535, 可选):

维持重定向连接的超时时间 (1-10秒，可选):

3

保存

设备与认证服务器之间的通信密钥:

恢复默认

保存

保存

线用户信息的更新时间间隔 (30-3600秒):

60

恢复默认

提示: 多个Vlan之间使用英文逗号分开，相连Vlan之间可以用“-”连接

Vlan List:

webIPURLHTTP(0-255)WebIP

SNMP-Inform, , Vlan List

80

1-67



IP

“ ”

1-68



IP

“ ”

“ ”

1-69

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：

FastEthernet 0/3

IP Only Mode ☒

保存

☐	序号	端口	IP Only Mode
☐	1	FastEthernet 0/1	YES
☐	2	FastEthernet 0/3	YES

全选

删除

“ ”

“ ”

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

保存

DHCP Snooping 信任端口设置

端口：

FastEthernet 0/1

保存

限速

DHCP Snooping配置信息

☐

端口

信任端口

■ DHCP Snooping

1-60

DHCP Snooping DHCP Snooping MAC

“ ”

■ DHCP Snooping

“ ”

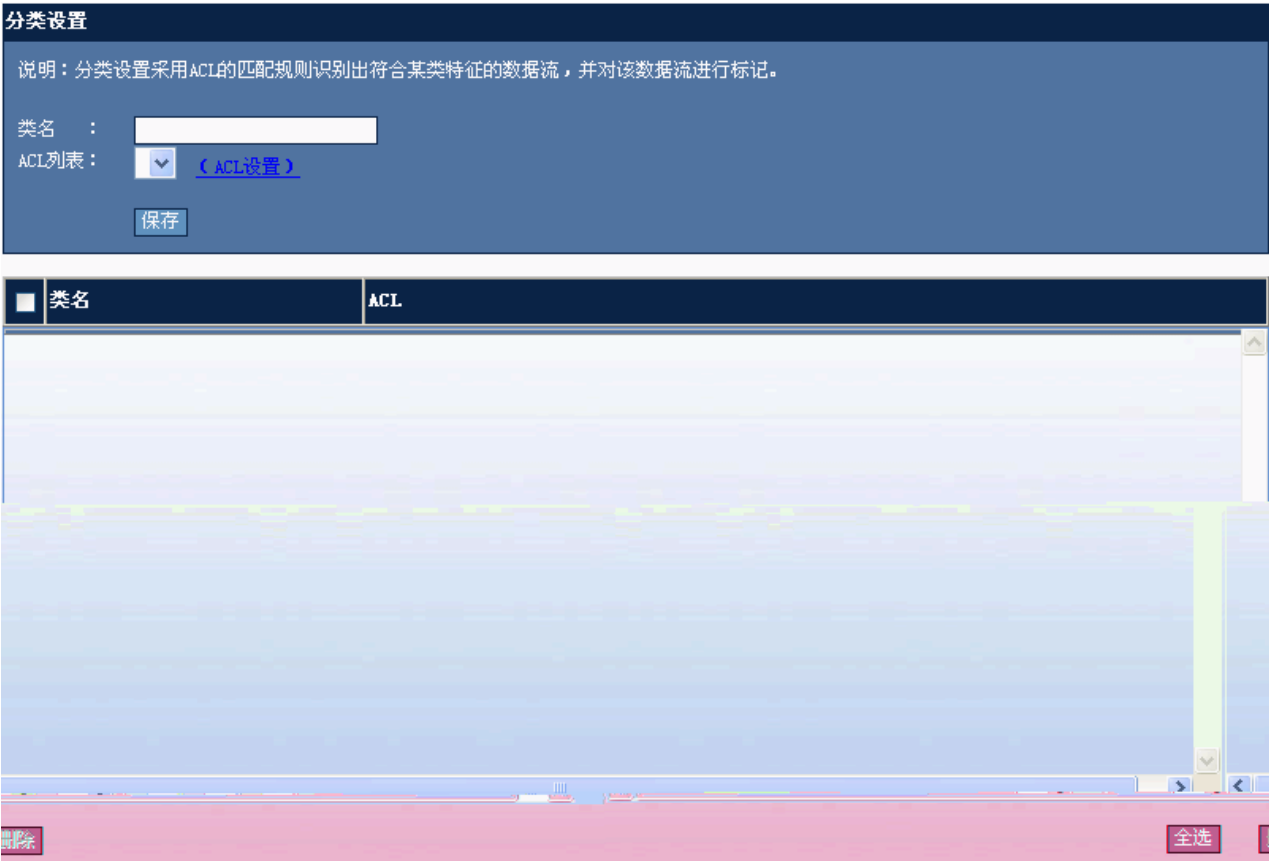
“ ”

1.7 QOS

1.7.1

“ ”

1-72

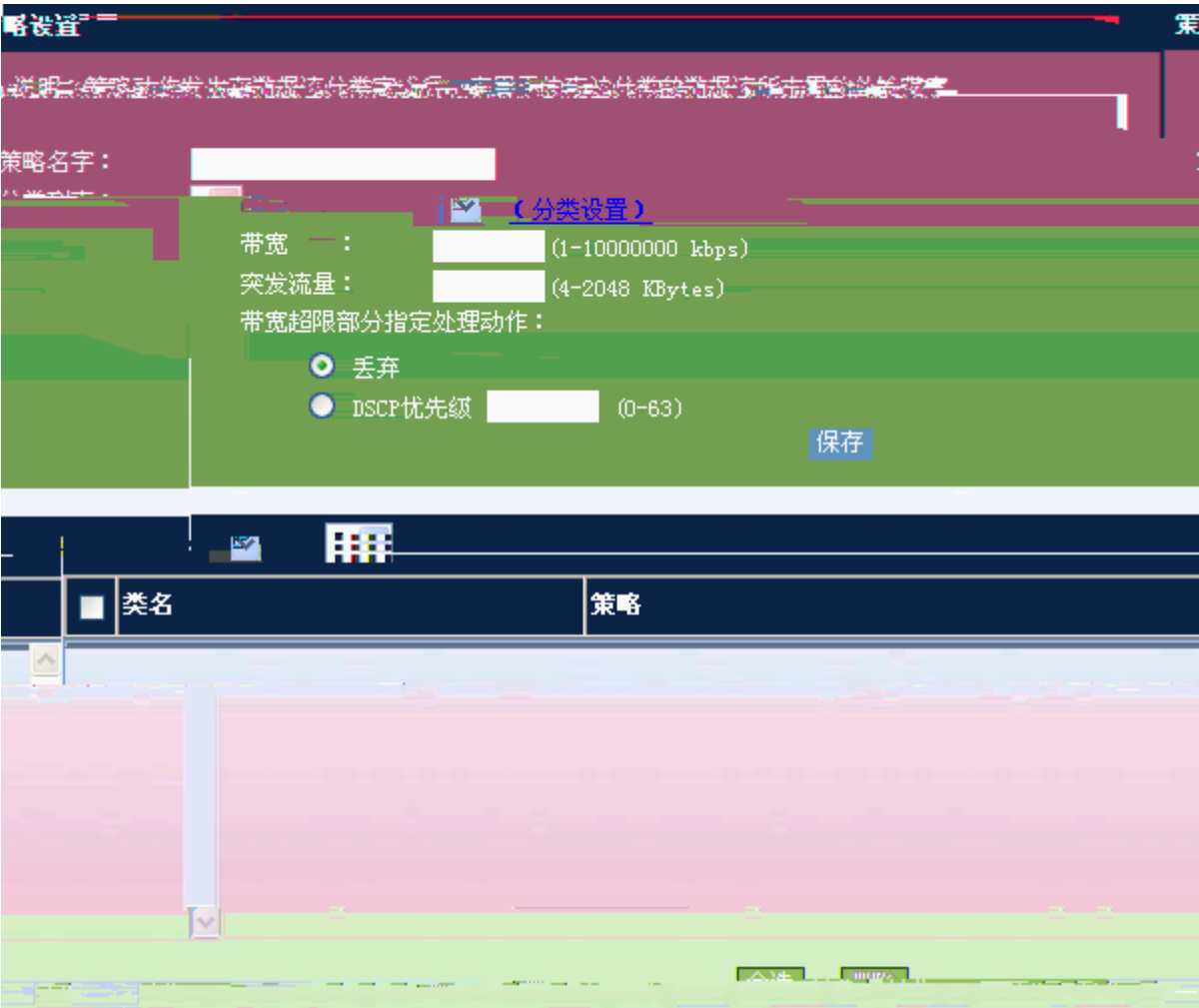


ACL “ ”
“ ”

1.7.2

“ ”

1-73



DSCP

“ ”

1.7.3

“ ”

1-74

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：

FastEthernet 0/1

策略列表：[（策略设置）](#)

限速方向：

输入限速

输出限速

保存

	端口	方向	策略名	信任模式	COS
☐	FastEthernet 0/1	-	-	-	-
☐	FastEthernet 0/2	-	-	-	-
☐	FastEthernet 0/3	-	-	-	-
☐	FastEthernet 0/4	-	-	-	-
☐	FastEthernet 0/5	-	-	-	-
☐	FastEthernet 0/6	-	-	-	-
☐	FastEthernet 0/7	-	-	-	-
☐	FastEthernet 0/8	-	-	-	-
☐	FastEthernet 0/9	-	-	-	-
☐	FastEthernet 0/10	-	-	-	-
☐	FastEthernet 0/11	-	-	-	-

全选

删除

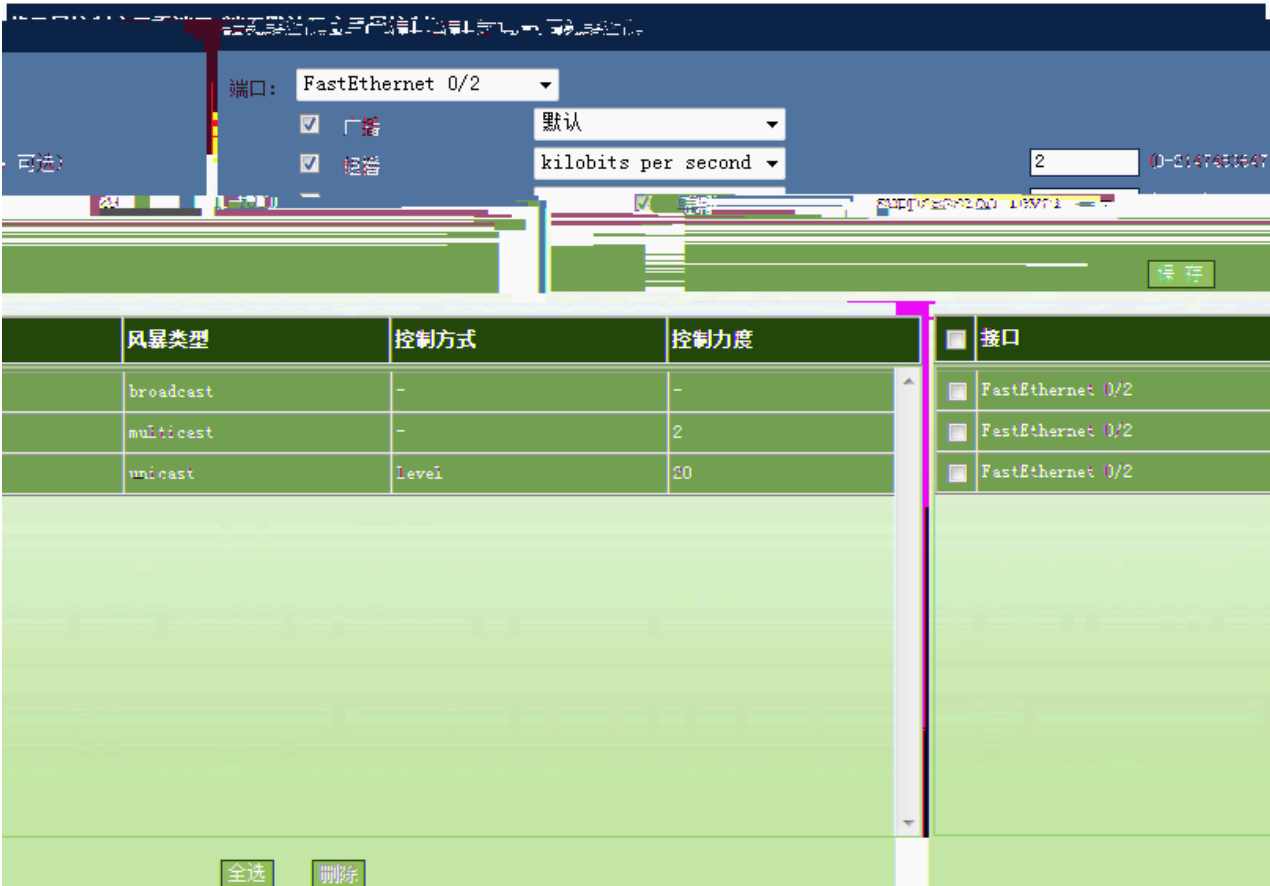
“ ”

“ ”

1.7.4

“ ”

1-75



“ ”
“ ”

1.7.5

“ ”

1-76



基本配置

安全地址

安全地址绑定

端口：

FastEthernet 0/1

地址：

1000.0000.0003

Vlan ID：

2

保存

接口	类型	MAC地址	Vlan ID
FastEthernet 0/2	-	1000.0000.0000	2
FastEthernet 0/5	sticky	1000.0000.0003	2

全选

删除

Mac VLAN ID “ ”
“ ”

基本配置

安全地址

安全地址绑定

端口：

FastEthernet 0/1

IP地址 (IPv4或IPv6):

1.2.3.3

将MAC及Vlan进行绑定到安全端口：☒

MAC地址：

1000.0000.0000

Vlan ID:

10

保存

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

全选

删除

Mac

“

”

IP

MAC

Vlan

“

”

1.8

1.8.1

“ ”

1-79

1.8.2

“ ”

1-80



```
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
!
```

1.8.3

“ ”

1-81

端口状态					
端 口	状 态	Vl an	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	900	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

1.8.4

“ ”

1-82

1.8.5

“ ”

1-83

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
*Feb 28 06:23:49: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 06:33:51: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 06:43:52: %ARPGUARD-4-SCAN: ARP scan was detected.
```

1.9.2 Telnet

“ Telnet ”

Telnet

1-86 Telnet

“ Telnet ”

Telnet

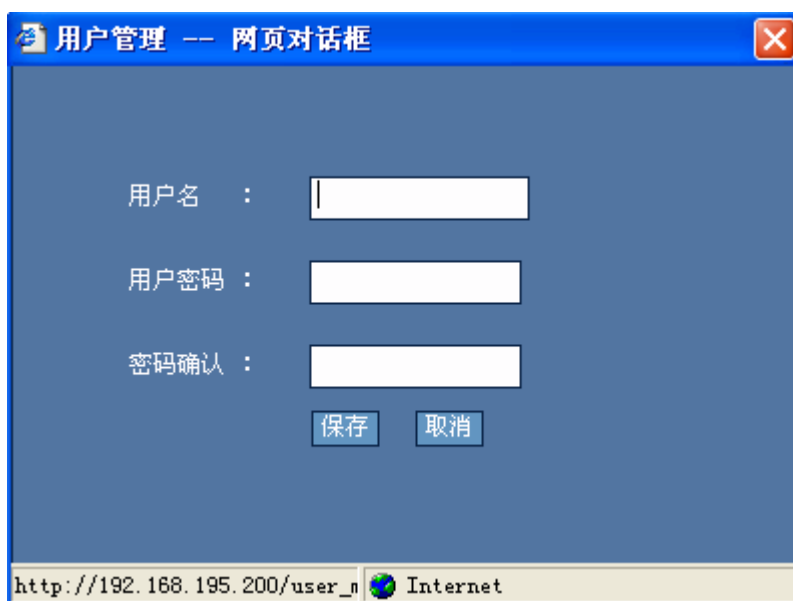
PC

Telnet

PC Telξ

“ ”

1-88



用户管理 -- 网页对话框

用户名 :

用户密码 :

密码确认 :

http://192.168.195.200/user_m Internet

“ ”

“ ”

“ ”

1-89

用户管理 -- 网页对话框

用户名 :

用户密码 :

密码确认 :

http://192.168.195.200/user_0 Internet

“ ”

a

— \$ —

■ 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

WEB Local Enable WEB WEB

■ Local

config

```
Ruijie#configure
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

WEB

```
Ruijie(config)#enable service web-server
```

WEB

Local

```
Ruijie(config)#ip http authentication local
```

15

```
Ruijie(config)#username admin password admin
```

```
Ruijie(config)#username admin privilege 15
```

IP

```
Ruijie(config)#interface vlan 1
```

```
Ruijie(config-if-VLAN 1)#ip address 192.168.100.1 255.255.255.0
```

■ Enable

config

```
Ruijie#configure
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

WEB

```
Ruijie(config)#enable service web-server
```

WEB

Enable

```
Ruijie(config)#ip http authentication enable
```

Enable

```
Ruijie(config)#enable password admin
```

IP

```
Ruijie(config)#interface vlan 1
```

```
Ruijie(config-if-VLAN 1)#ip address 192.168.100.1 255.255.255.0
```

■ 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-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
```