



© 2014



RGOS®

RGNOS®



锐捷®

Â <http://www.ruijie.com.cn/>

Â <http://webchat.ruijie.com.cn>

8:30 6 “ ”

3.

Â

Â

Â

```

WEB      G      ^      IE~      ^
WEB      WEB  L      WEB      ч  |  ^ WEB  L      3~      4      ^
1 WEB      ^      3      ~      ~      WEB      IE ^

```

```

      G      WEB      WEB      |  H      WEB      H      ^      PC
≠ 1      y·q·è      ||      ~      à IPAD
      '      IE6.0 à IE7.0 à IE8.0  Лб  ↓  |  ы  IE      ~      ý      à maxthon      ^ G      è
WEB      ~  1      Ъ
|      '      |      н  1024*768 à 1280*1024  ↓  1440*960      è  |      Ю      E      1      a
à a      ^

```

```

H      í  || WEB  L ^      Ω ^
H      WEB      а  ^      Лб Local      Enable      ~      ±~      1
Лб  ó WEB      ^
H      IP      ^      о  н  web      ^

```

```

ЛбЮwR      L      3      ^

```

ó config

```

Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.

```

```

WEB  L

```



```
Ruijie#configure
```

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

```
WEB  1
```

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

```
WEB          2 Enable  ^      3      4 a      5 ~
```

```
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 192.168.195.200 255.255.255.0
```

```
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      //  1 WEB  2
```

```
!
```

```
!
```

```
interface VLAN 1
```

```
ip address 192.168.195.200 255.255.255.0 //      IP
```

```
no shutdown
```

```
!
```

```
!
```

```
line con 0
```

```
line vty 0 4
```

```
login
```

```
!
```

```
!
```

```
end
```

```
WEB
```

```
Enable
```

```
Enable
```

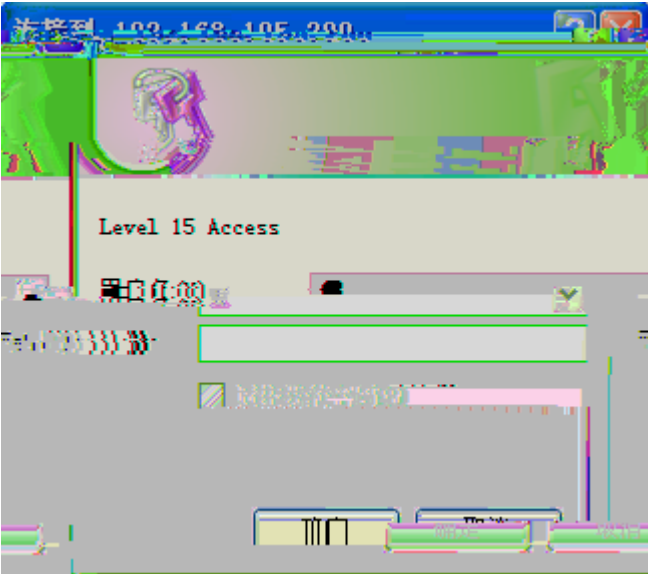

è ò IP ~ http://192.168.195.200 ‡ ò IO ‘

1-1]



‡ † L ~ ~ è ò ¨ ä Â

1-2

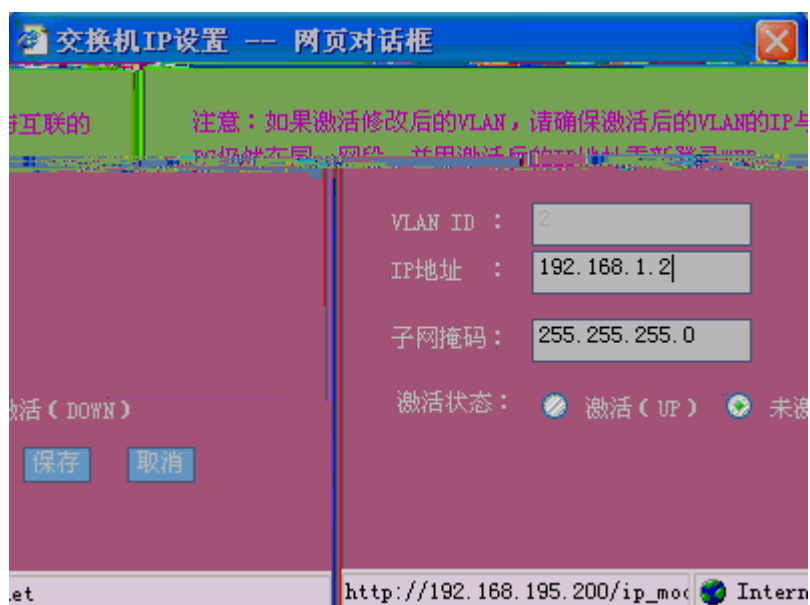


¶ ‡ ò WEB Ÿ ~ IO ‘

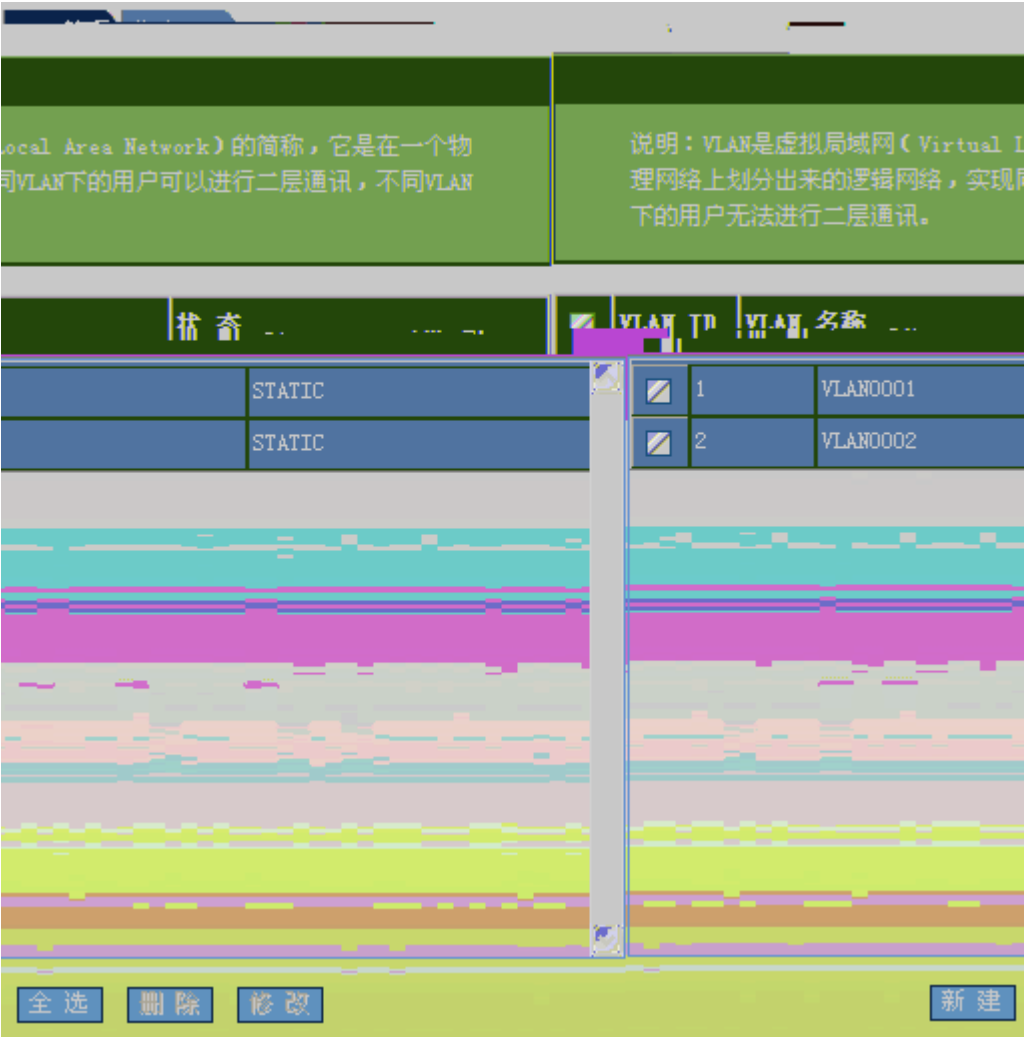
1-3 WEB

/1 ý

☐ ξ M



1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100



2-4 VLAN

VLAN管理 -- 网页对话框

VLAN ID :

(1-4094)

VLAN 名称 :

(可选)

保存

取消

ω VLAN ID

VLAN "

^ / ~ ±

Γ ϛ

E

G

Â

Π ±

VLAN

VLAN

∃ Â

Γ ' Γ

VLAN

è

±

Γ Γ

E

G

Â

g ' g

VLAN

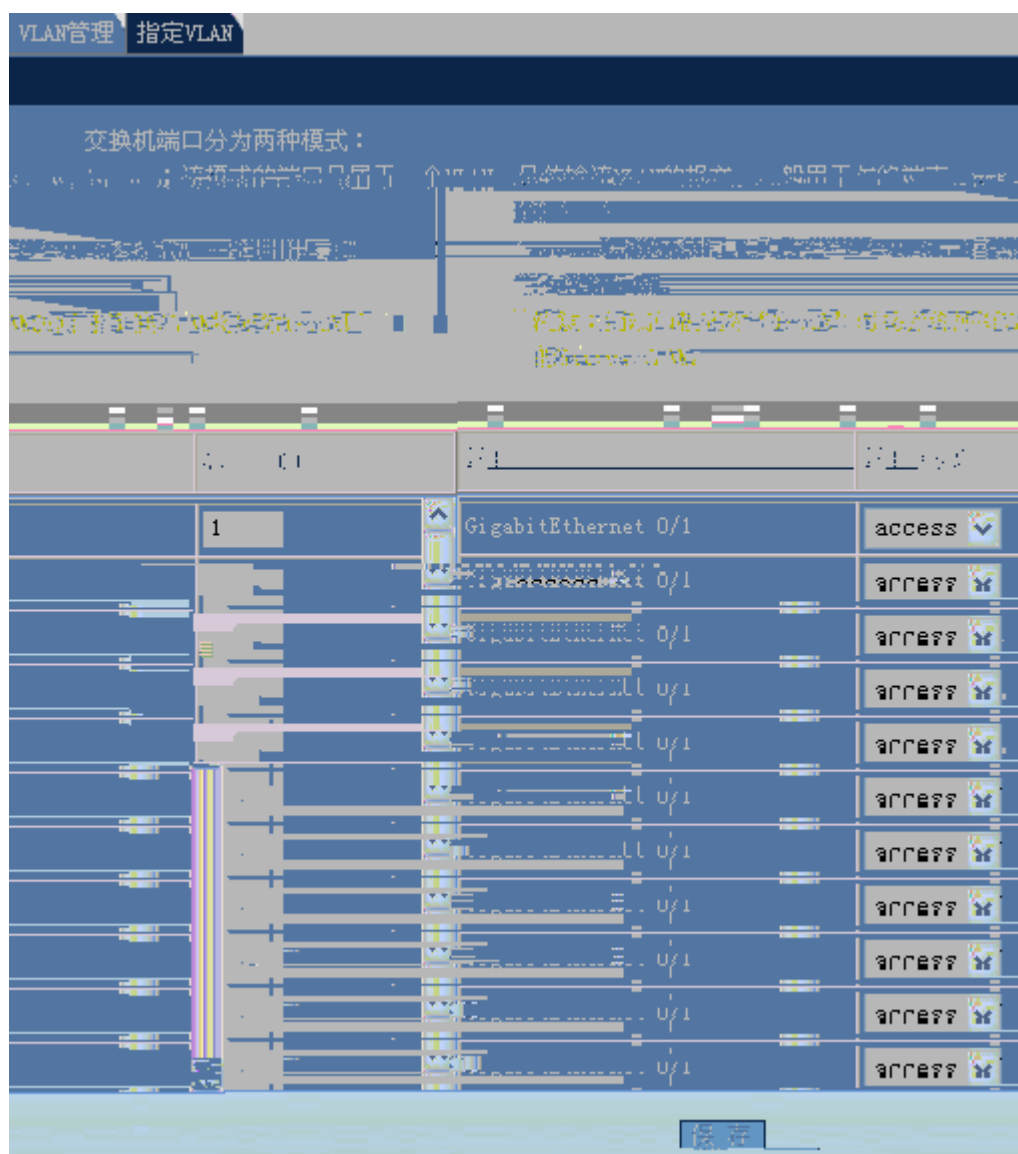
/ 9

è \$ 1

±

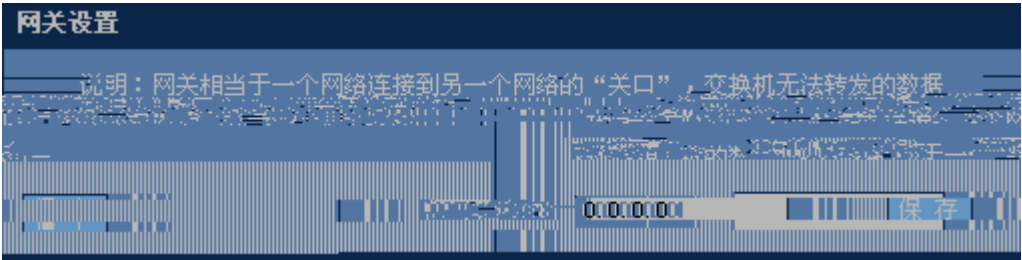
Γ

è



VLAN ID	IP	MAC	Host
1	192.168.1.1	000000000000	Switch
2	192.168.2.1	000000000000	Switch
3	192.168.3.1	000000000000	Switch
4	192.168.4.1	000000000000	Switch
5	192.168.5.1	000000000000	Switch
6	192.168.6.1	000000000000	Switch
7	192.168.7.1	000000000000	Switch
8	192.168.8.1	000000000000	Switch
9	192.168.9.1	000000000000	Switch
10	192.168.10.1	000000000000	Switch
11	192.168.11.1	000000000000	Switch
12	192.168.12.1	000000000000	Switch
13	192.168.13.1	000000000000	Switch
14	192.168.14.1	000000000000	Switch
15	192.168.15.1	000000000000	Switch
16	192.168.16.1	000000000000	Switch
17	192.168.17.1	000000000000	Switch
18	192.168.18.1	000000000000	Switch
19	192.168.19.1	000000000000	Switch
20	192.168.20.1	000000000000	Switch
21	192.168.21.1	000000000000	Switch
22	192.168.22.1	000000000000	Switch
23	192.168.23.1	000000000000	Switch
24	192.168.24.1	000000000000	Switch
25	192.168.25.1	000000000000	Switch
26	192.168.26.1	000000000000	Switch
27	192.168.27.1	000000000000	Switch
28	192.168.28.1	000000000000	Switch
29	192.168.29.1	000000000000	Switch
30	192.168.30.1	000000000000	Switch
31	192.168.31.1	000000000000	Switch

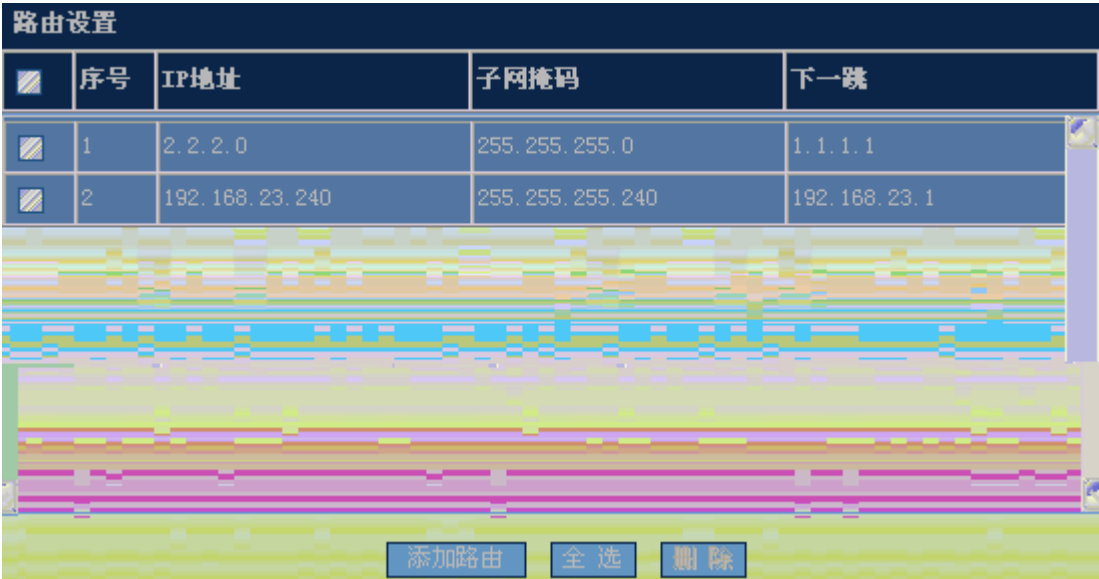
$$\Gamma \cong \Omega \times \mathbb{Z} \times \hat{A}$$
 τ_{Ω} 2-7 τ_{Ω}



在配置网关时，需要指定网关的IP地址。

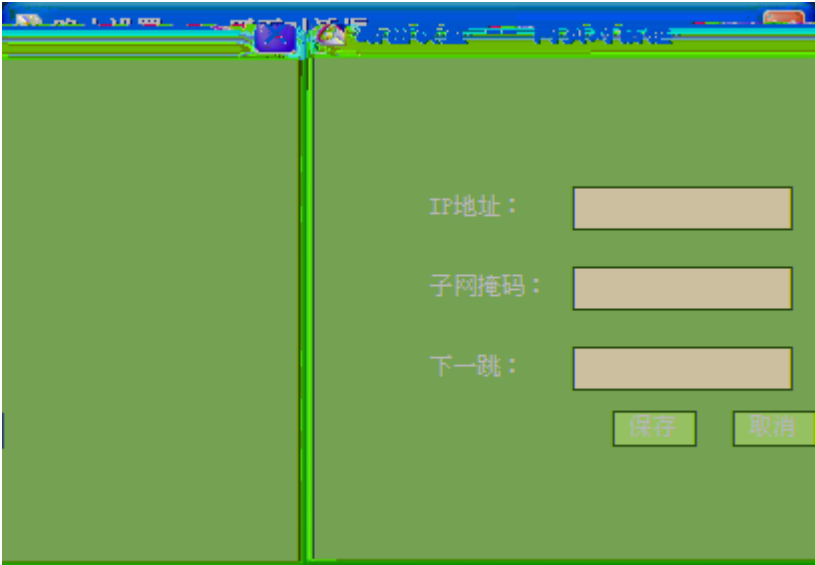
在配置网关时，需要指定网关的IP地址。

2-8



在配置路由时，需要指定路由的IP地址、子网掩码和下一跳。

2-9



IP 地址 子网掩码 下一跳 保存 取消

VRRP 组 ID 优先级 认证 认证文本

2-11 VRRP

VRRP设置 -- 网页对话框

接口： VLAN 1

组号： 1

IP地址：

通告发送间隔 (1-255秒)：

优先级 (1-254)：

启用抢占模式： ☒

被监视接口： 插入

保存 取消

输入限速

输出限速

端口输入限速设置

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	输入速率限制 (0.1-1000000,单位:1000000)	瞬时速率限制 (0.1-1000000)	
GigabitEthernet 0/1			GigabitEthernet 0/1
GigabitEthernet 0/2			GigabitEthernet 0/2
GigabitEthernet 0/3			GigabitEthernet 0/3
GigabitEthernet 0/4			GigabitEthernet 0/4
GigabitEthernet 0/5			GigabitEthernet 0/5
GigabitEthernet 0/6			GigabitEthernet 0/6
GigabitEthernet 0/7			GigabitEthernet 0/7
GigabitEthernet 0/8			GigabitEthernet 0/8
GigabitEthernet 0/9			GigabitEthernet 0/9
GigabitEthernet 0/10			GigabitEthernet 0/10
GigabitEthernet 0/11			GigabitEthernet 0/11

保存

取消全部输入限速

1) 。

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

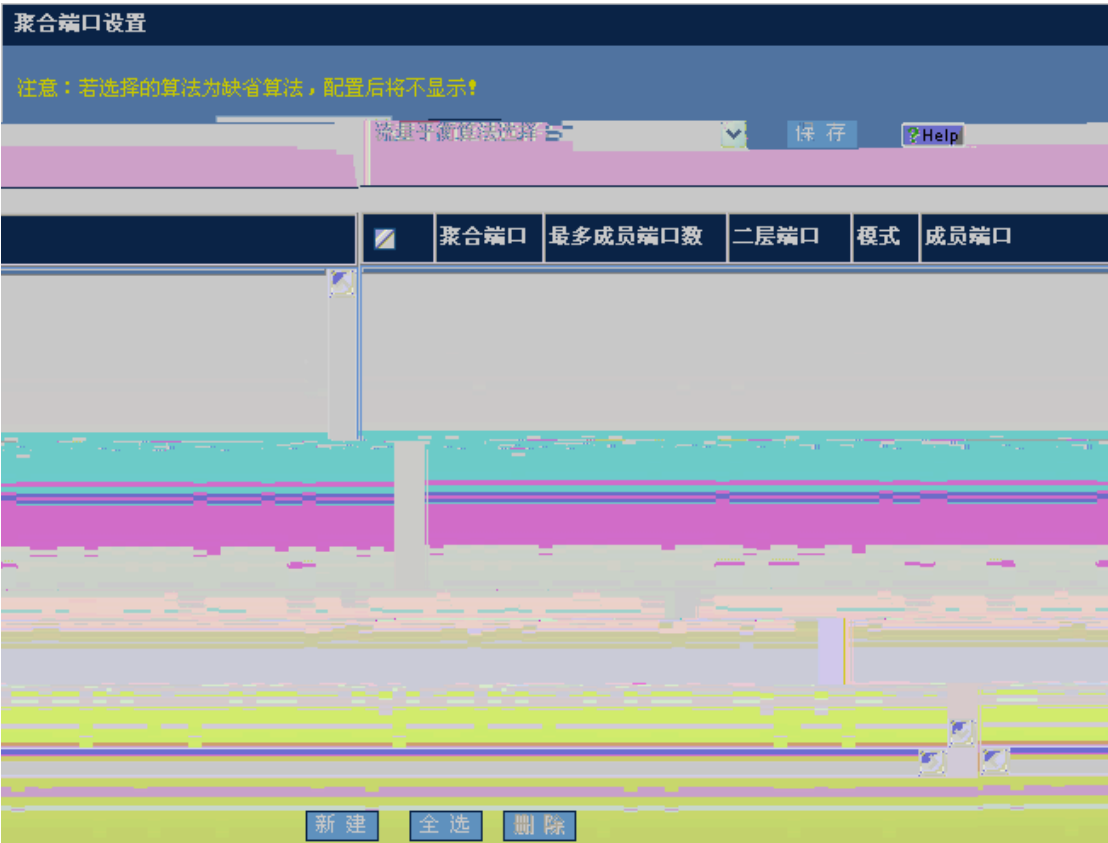
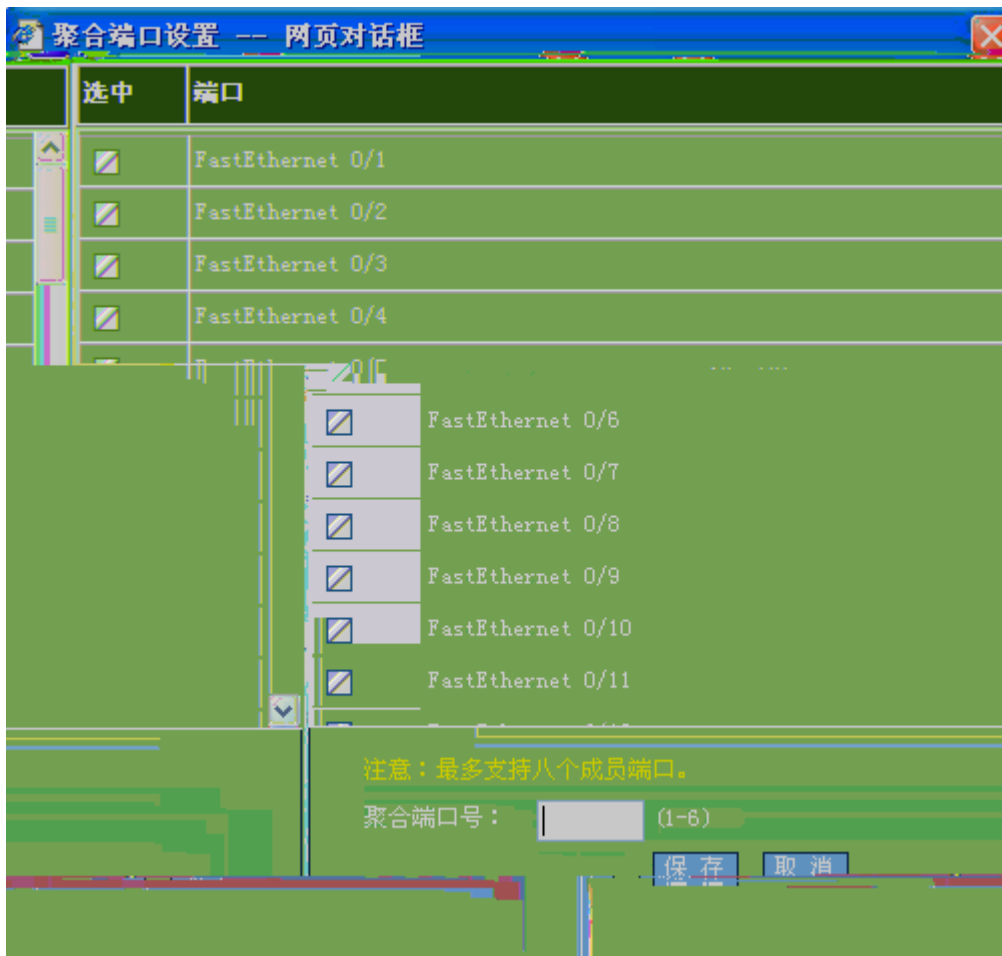
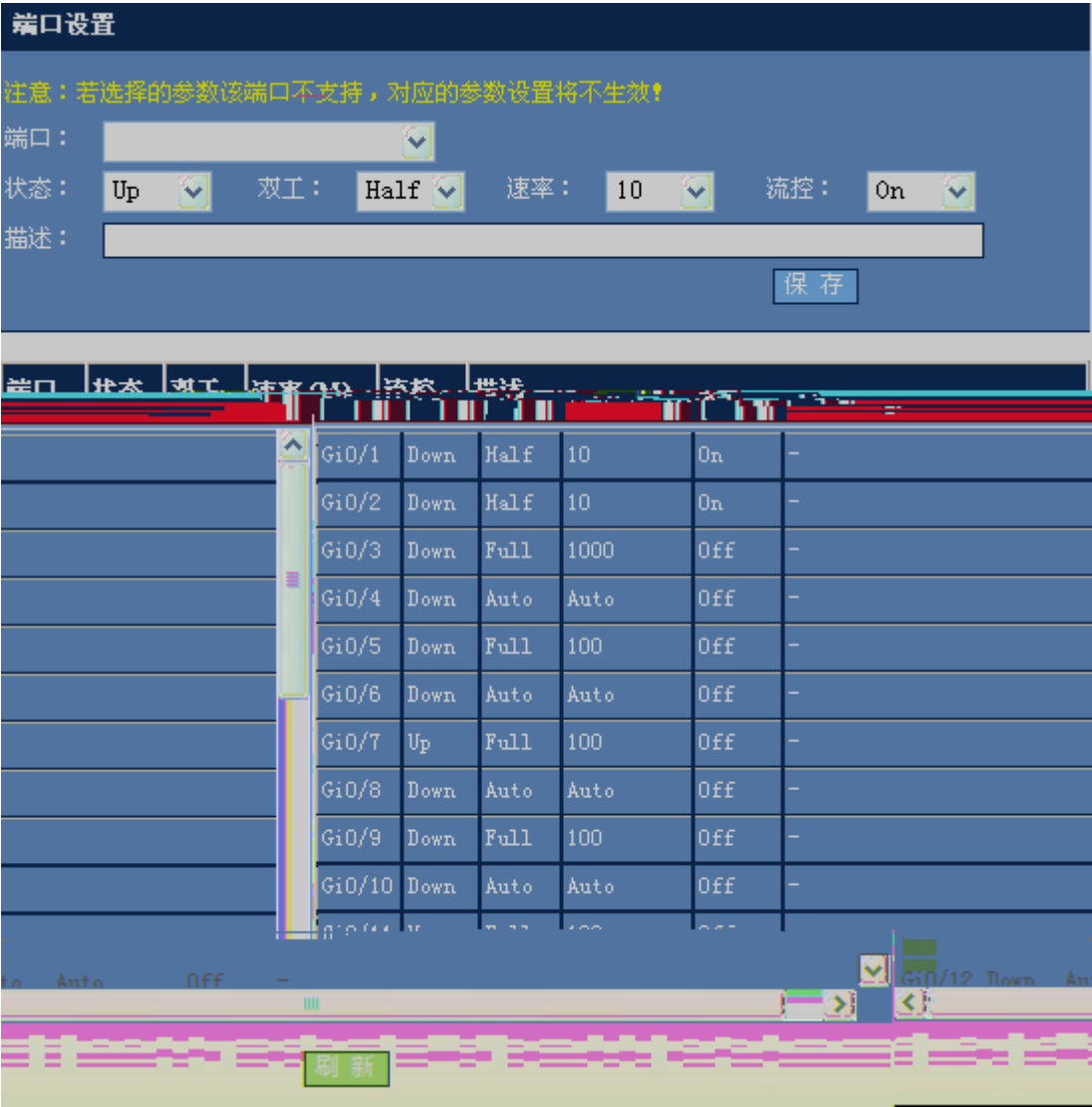


图 2-16 聚合端口设置



2-17

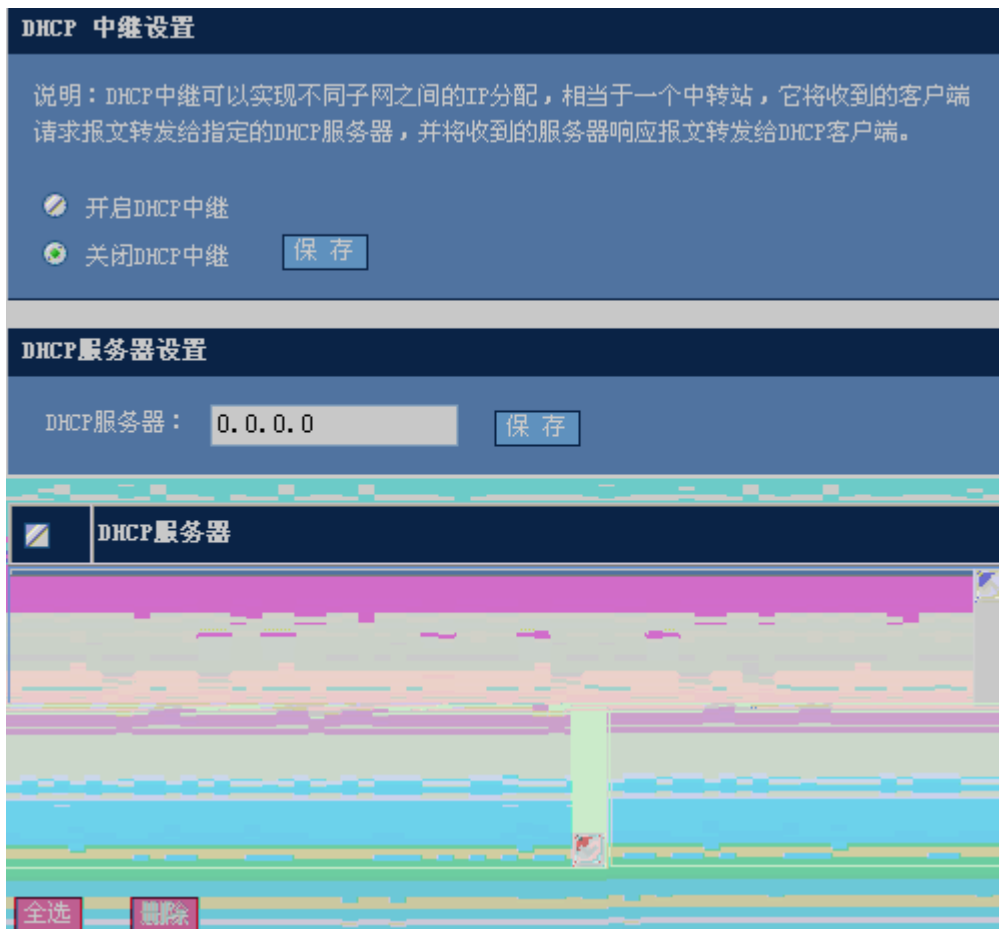


√ ± è ~ √ ± r q L G Â √ a ~ √
a Â

√ r DHCP è L G ∏ Â

DHCP è

2-18 DHCP è



í /Ω DHCP è

/Ω DHCP è π ~ è 、 ı~ İ đ E G Â

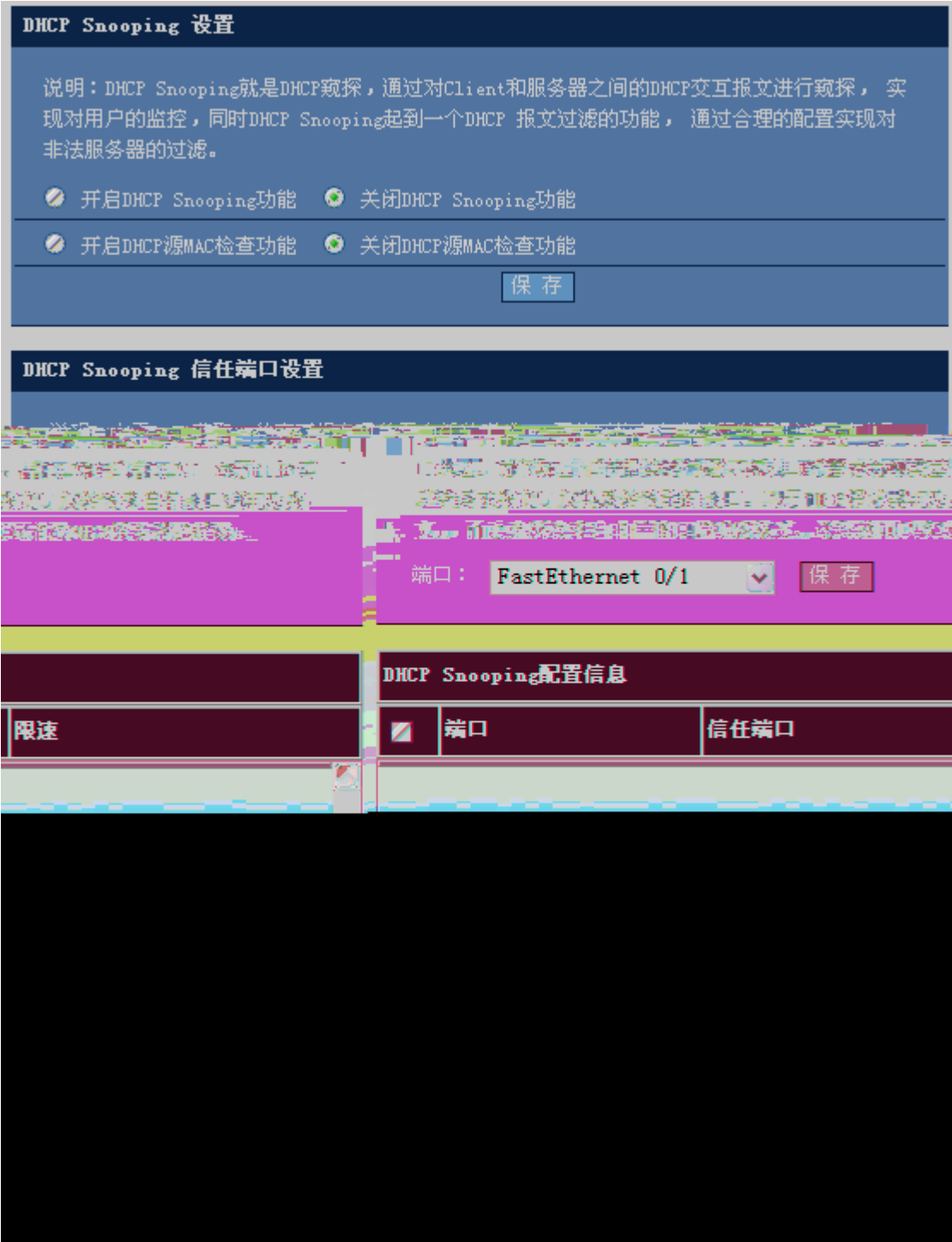
DHCP E

DHCP E ı~ İ đ E G Â π ı İO è Â İ DHCP E ~ è ı İ đ E G Â

、 İ DHCP Snooping E G π Â

DHCP Snooping

2-19 DHCP Snooping



DHCP Snooping

í DHCP Snooping π DHCP Snooping MAC π ~ è ´ ± P d E G Â

DHCP Snooping a´ J

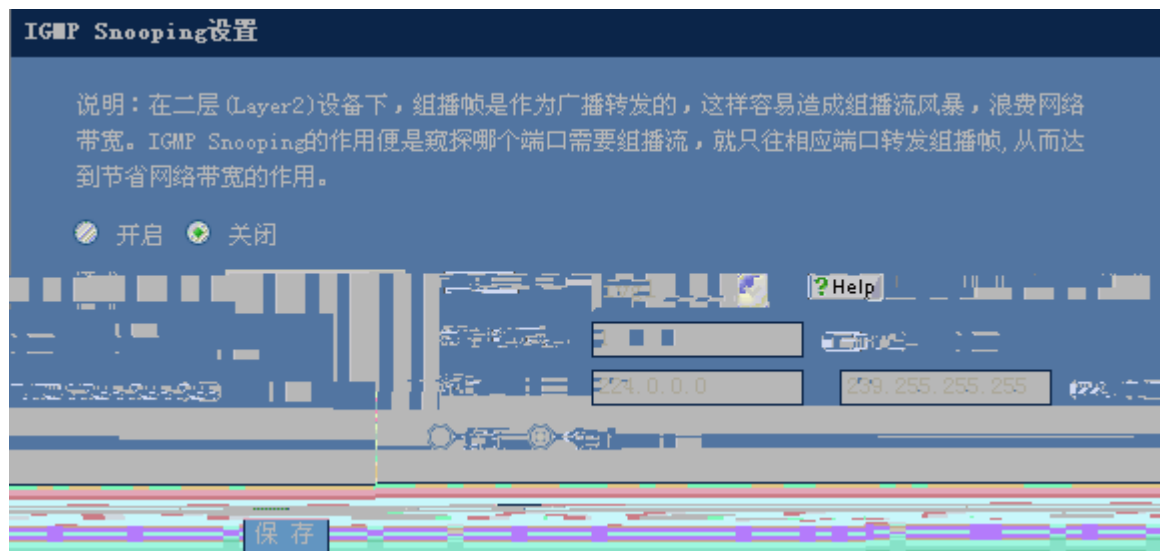
ñ a´ J ± P d E G ~ π ± IO a Â í a´ J~

è ± P d E G Â

IGMP Snooping 配置

IGMP Snooping

2-20 IGMP Snooping



IGMP Snooping 配置

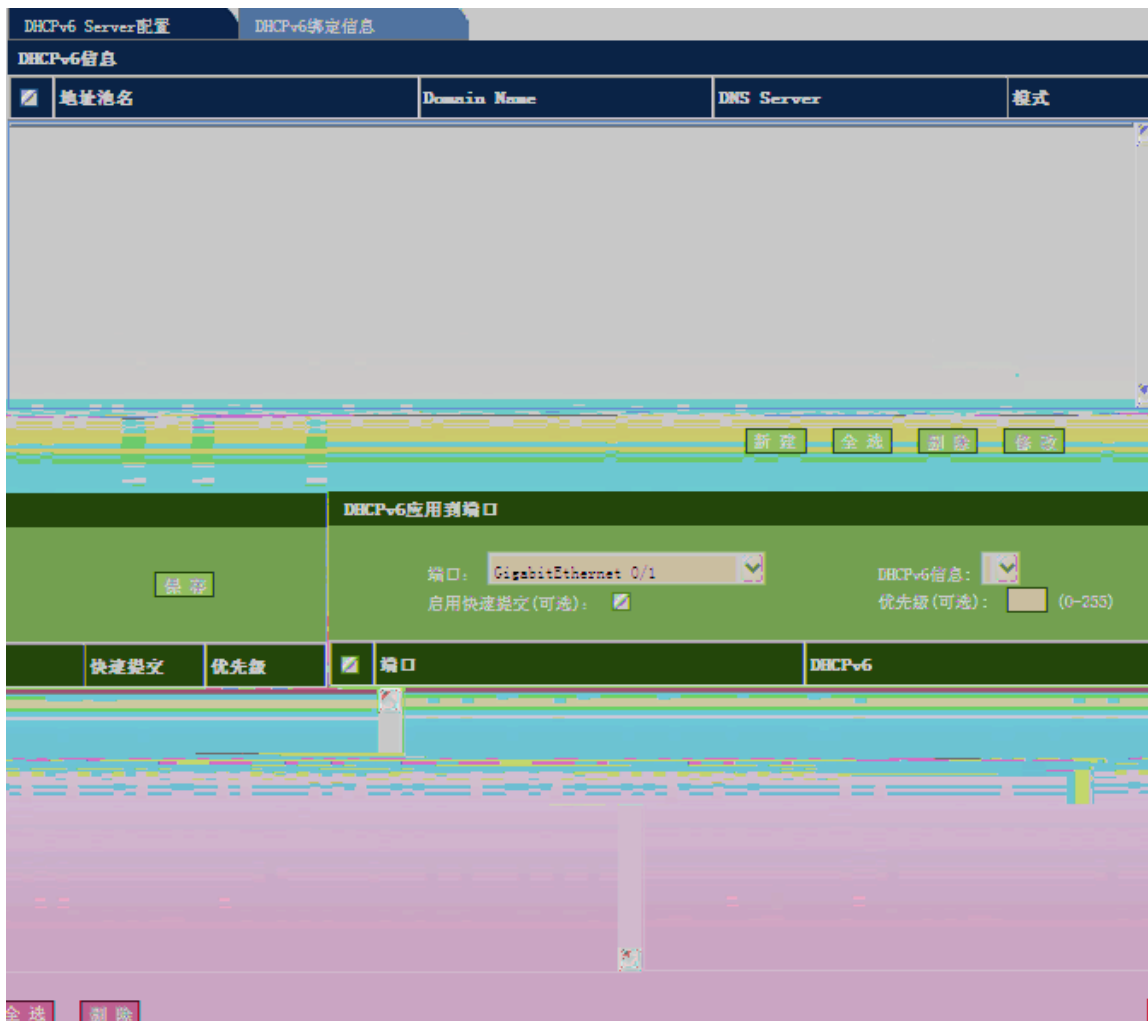
说明：在二层 (Layer2) 设备下，组播帧是作为广播转发的，这样容易造成组播流风暴，浪费网络带宽。IGMP Snooping 的作用便是窥探哪个端口需要组播流，就只往相应端口转发组播帧，从而达到节省网络带宽的作用。

开启 关闭

Help

224.0.0.0 229.255.255.255

保存



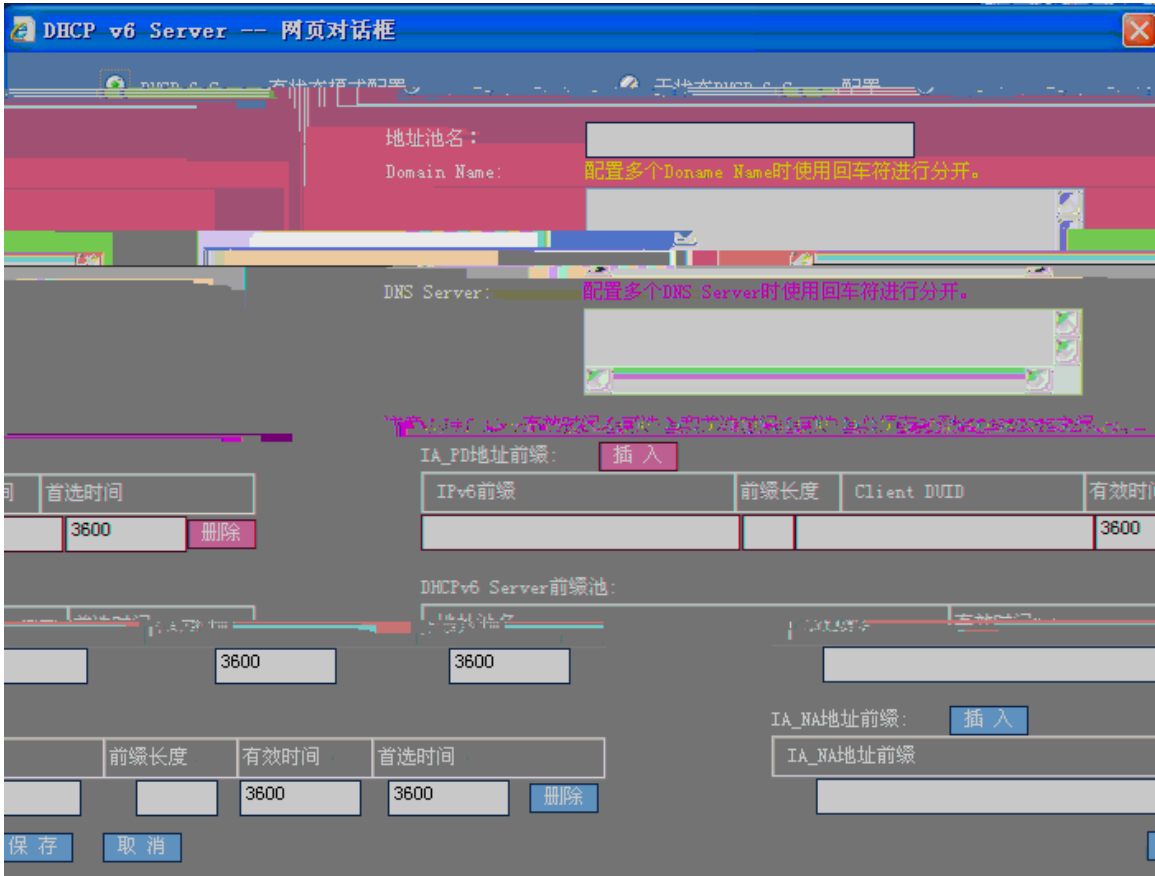
1) DHCPv6 Server

Э' | й DHCPv6 Server Ω ~ / Л DHCPv6 Server ä | 9 о~ Ю' | й DHCPv6
↑ / Â

DHCPv6 L

У э DHCPv6 L ~ I' E ~ Ю '

2-22 DHCPv6 L



DHCPv6 DHCPv6 A

 @ " ä " DNS L " ~ ^ ü A_NA ä IA_TA ä IA_PD B

 r ó L r IA r L r m IA r A r q L

 G A

DHCPv6 Server IO

2-23 DHCPv6 Server



 @ " ä " DNS L " ~ r q L G A

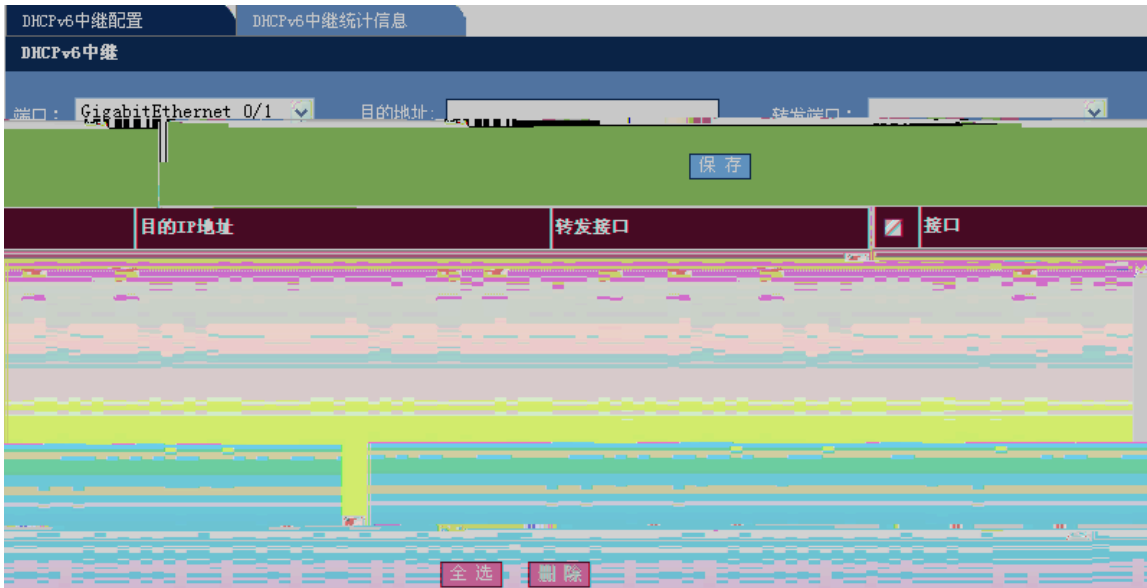
 r DHCPv6 Server

,

1

9

2-



•

17

2

2

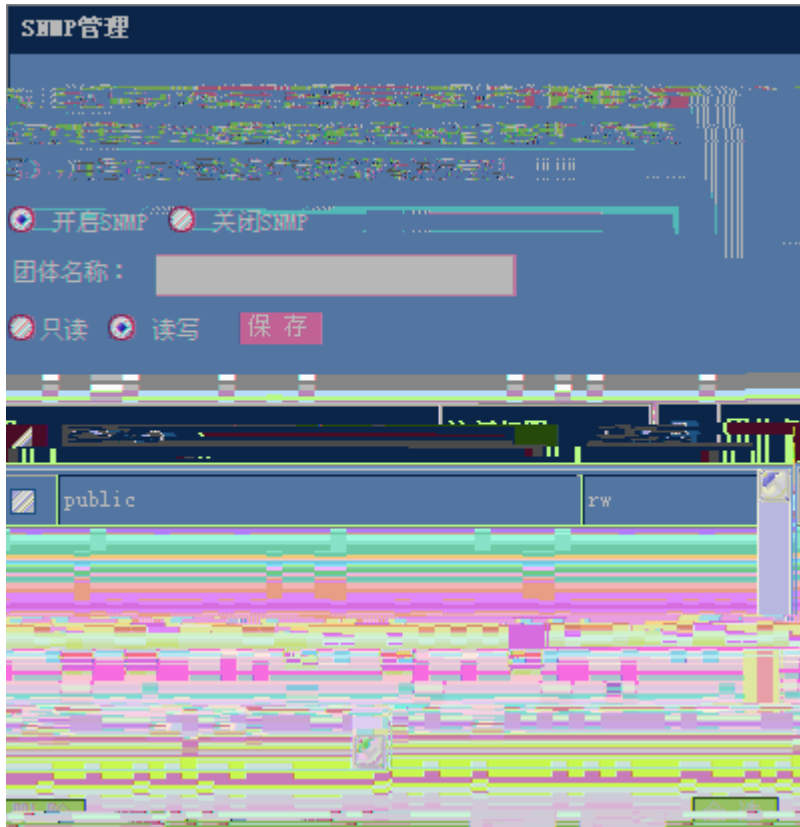


DHCPv6 a A r 9 E a ~ r L ~ G a A

 ` r STP L G 77 A

STP `

2-28 STP

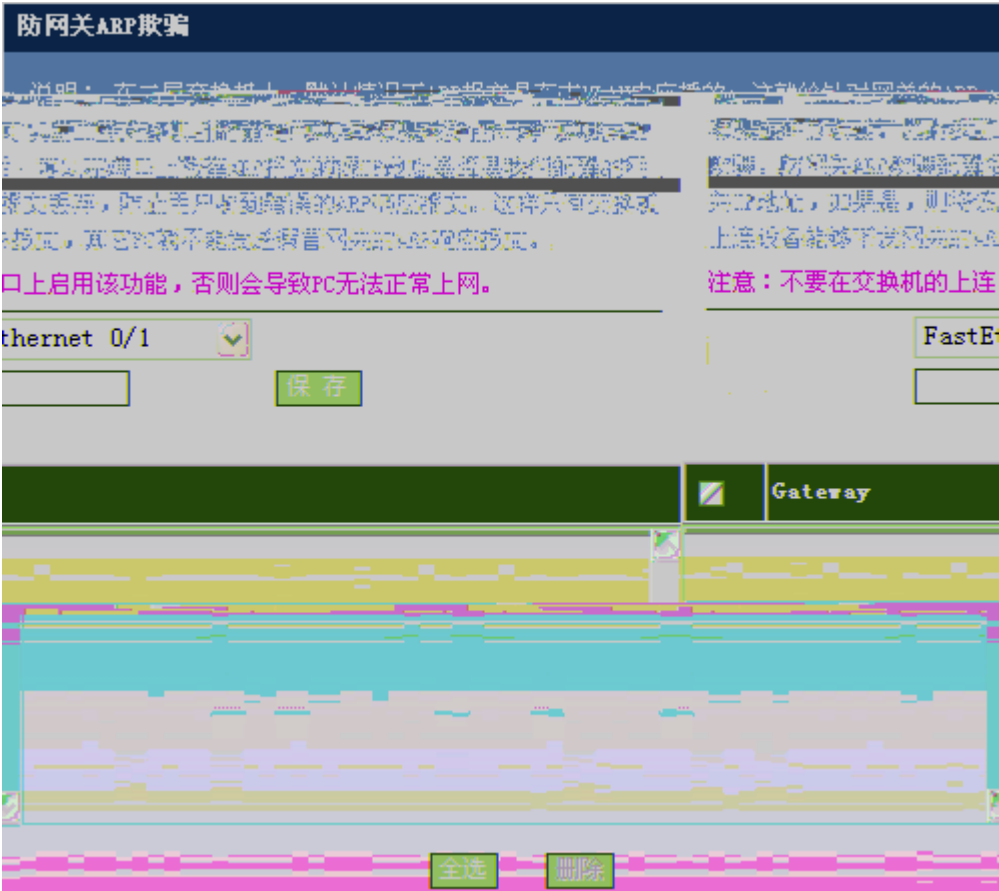


í SNMP π ~ Í í SNMP L` ~ Λ Λ
 ✓ í ~ Í q L G Â Ω SNMP π ~
 、 í ~ Í q L G Â Ĩ E ~
 í Í Ĩ L G Â
 E ~ à ĩ ~
 Í Ω SNMP L
 è Ĩ

、 I ARP E G 11 A

ARP

3-1 ARP



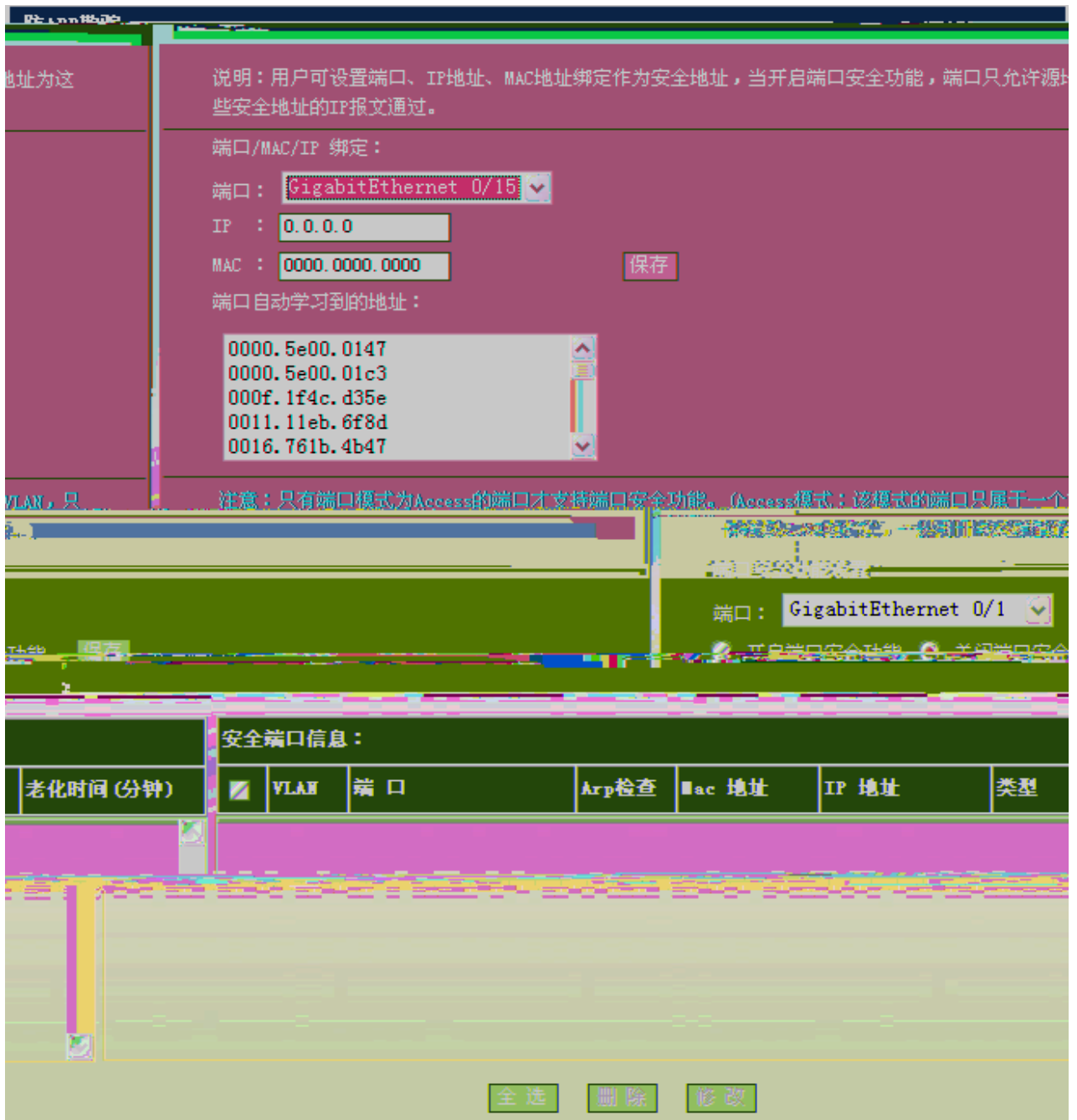
è M~ ó ARP ± I q E G ~ y 9 M 1 9 ARP ~ 1

ARP è 1 ARP ~ I1 E G A

、 I ARP E G 11 A

ARP

3-2 ARP



端口/MAC/IP

端口/MAC/IP 绑定： 端口： GigabitEthernet 0/15 IP： 0.0.0.0 MAC： 0000.0000.0000 保存

端口自动学习到的地址：

0000.5e00.0147
0000.5e00.01c3
000f.1f4c.d35e
0011.11eb.6f8d
0016.761b.4b47

注意：只有端口模式为Access的端口才支持端口安全功能。(Access模式：该模式的端口只属于一个VLAN，只...

端口： GigabitEthernet 0/1

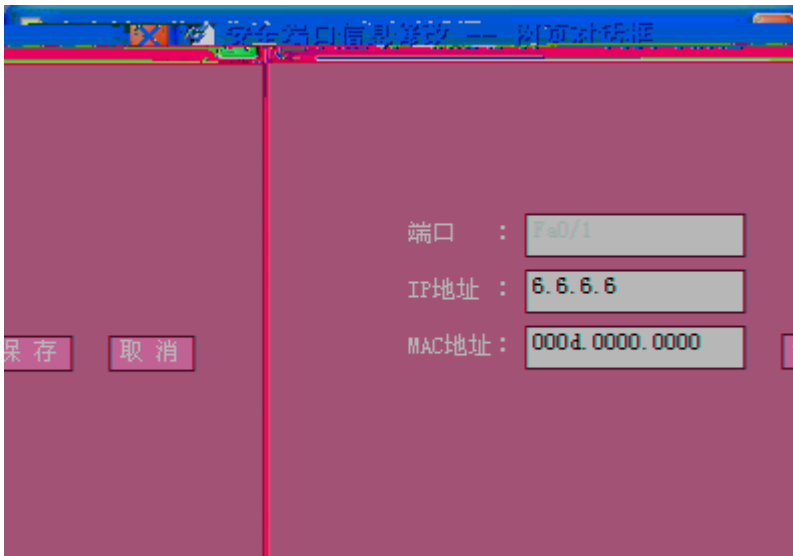
安全端口信息：

老化时间 (分钟)	☒ VLAN	端 口	☒ Arp检查	☒ Mac 地址	IP 地址	类型

全选 删除 修改

3-3 安全端口配置修改

3-3 安全端口配置修改



3-4 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。

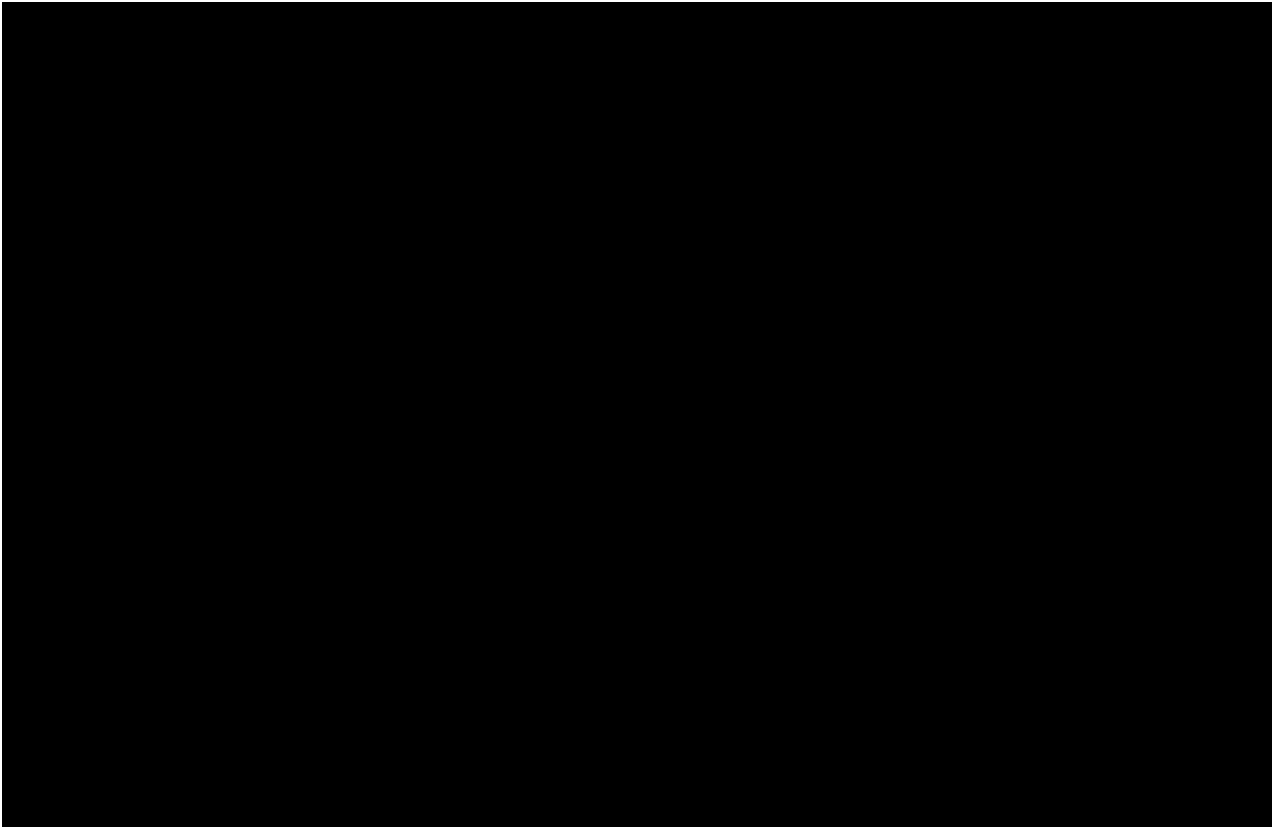
3-4 ARP

3-4 ARP



3-4 ARP 检查设置

3-5 ACL



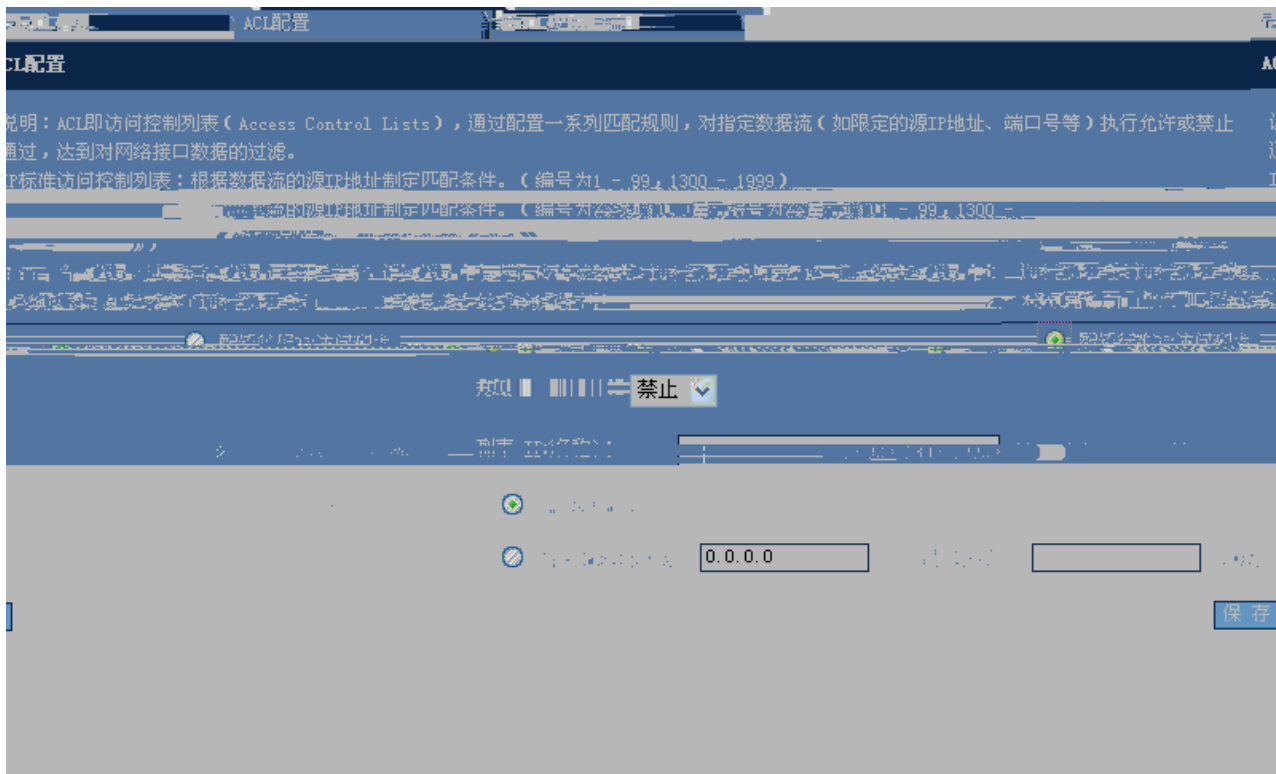
ACL a_l

ACL a_l ACE Â ACE' ACL a_l y ACL " è è ACL z[~] f_v è
 ACL I' L z[~] è ACE' I' L G Â I'
 ACL[~] I' L z[~] è ACE' I' L G Â

ACL

ñ IP " I' ñ IP " L` ~ Ю ñ ñ IP " '

3-6 ñ IP "



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。

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）

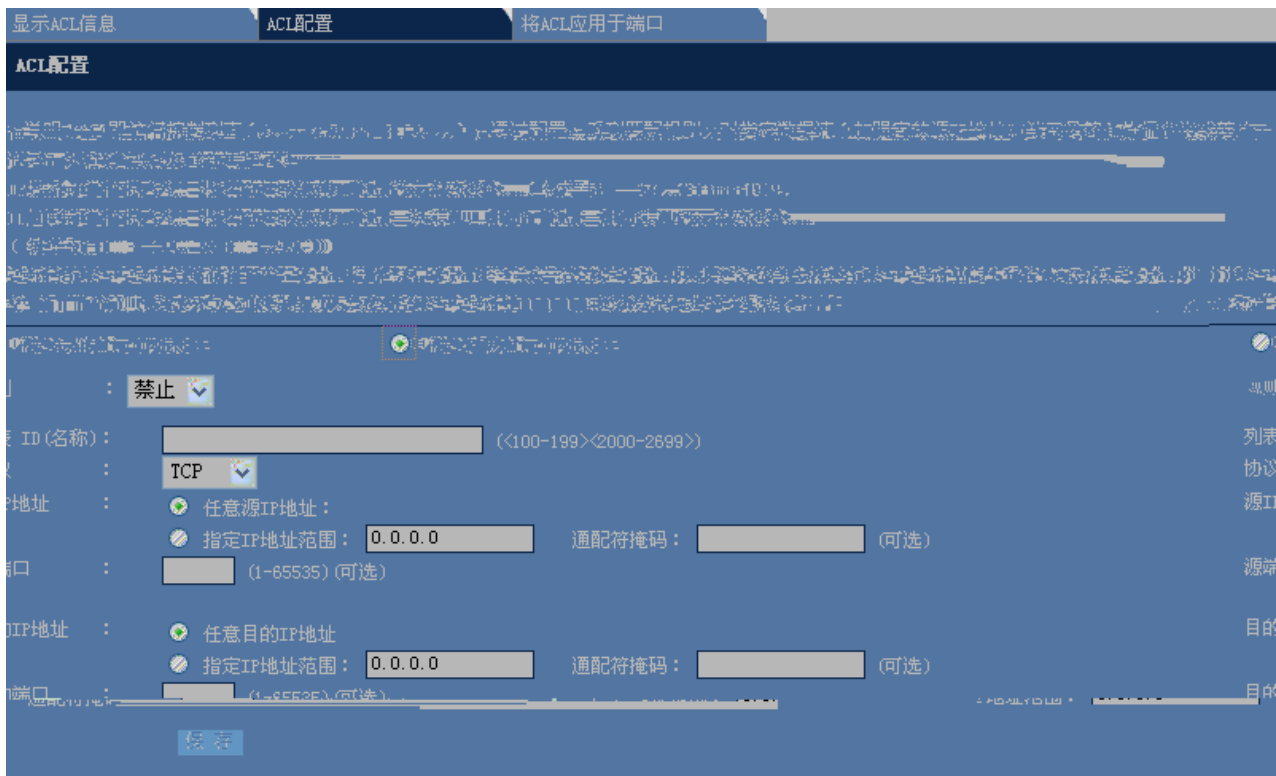
扩展访问控制列表：根据数据流的源IP地址制定匹配条件。（编号为2000 - 2999，编号为3000 - 3999，13000 - 13999）

配置ACL时，请按照以下步骤操作：

1. 创建ACL：在ACL配置页面，选择“标准访问控制列表”或“扩展访问控制列表”，输入ACL ID、名称、状态和动作，点击“保存”。

2. 应用ACL：在接口配置页面，选择要应用的接口，输入ACL ID，点击“应用”。

3. 验证配置：在配置完成后，可以通过“配置验证”功能验证配置是否正确。



禁止源IP地址为任意IP地址的目的IP地址为任意IP地址的TCP连接。

~ 配置 ACL 规则：TCP 到 UDP 到 IP 到 ICMP

IP 地址为任意IP地址的目的IP地址为任意IP地址的TCP连接。

~ 配置 ACL 规则：TCP 到 UDP 到 IP 到 ICMP

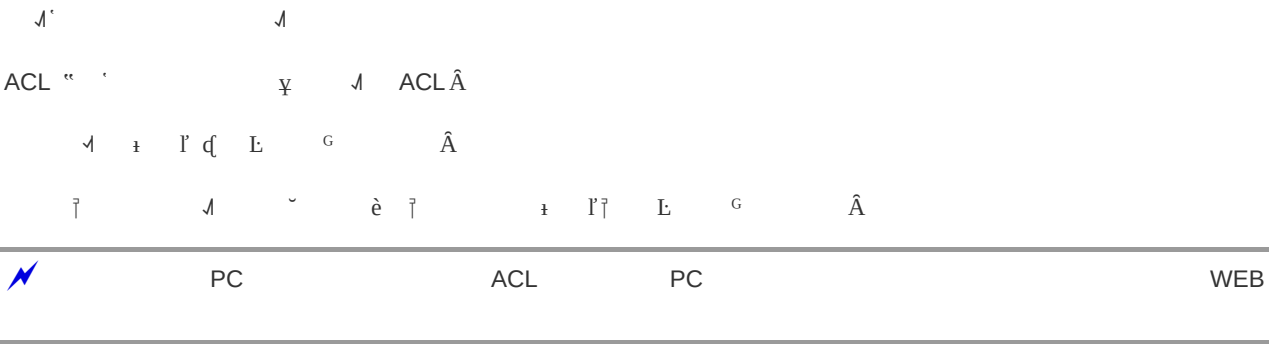
IP 地址为任意IP地址的目的IP地址为任意IP地址的TCP连接。

~ 配置 ACL 规则：TCP 到 UDP 到 IP 到 ICMP

~ 配置 ACL 规则：TCP 到 UDP 到 IP 到 ICMP

~ 配置 ACL 规则：TCP 到 UDP 到 IP 到 ICMP

3-8 ACL 规则配置



4-3

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

4' 4 Â

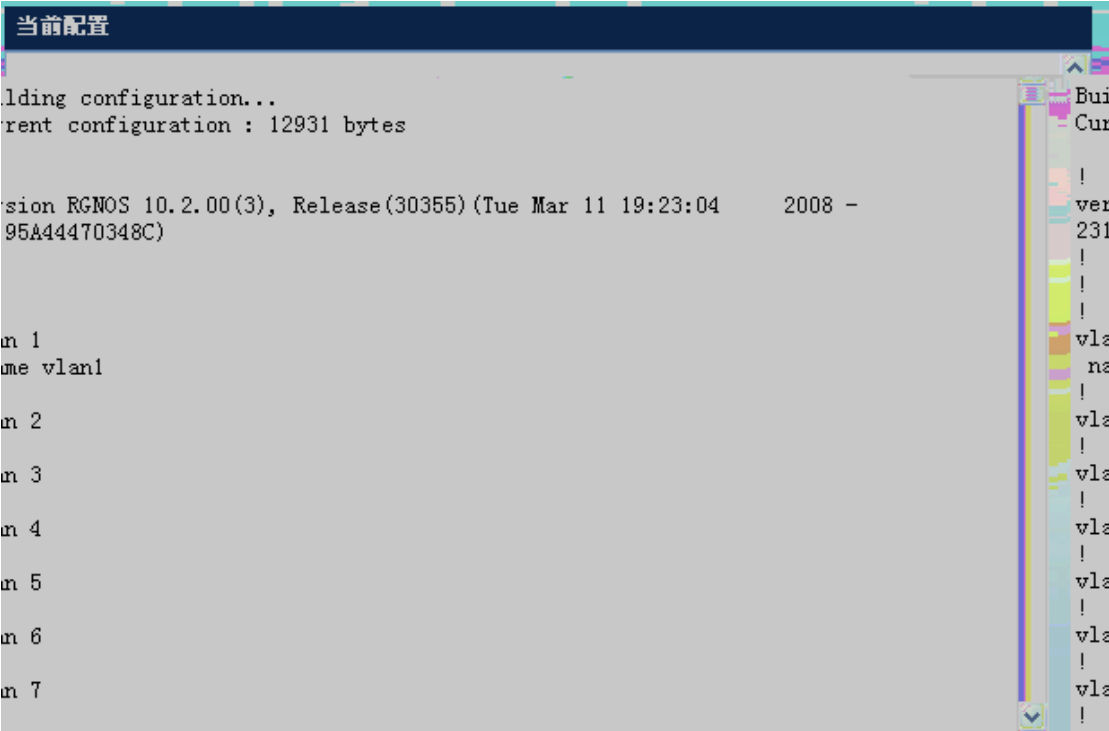
“ ’ ı 4 ~ “ ñ ~ ”I Â

ã' ã Â

4 ± İ ç L G Â ĩ 4 ~ è ĩ ± İ ĩ L

G Â

Г а L G П А
 а
 5-1 а я М
 5-1



5-3

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

、 ƒ ʹ E ʒ ʔ Ā

ʹ ʹ

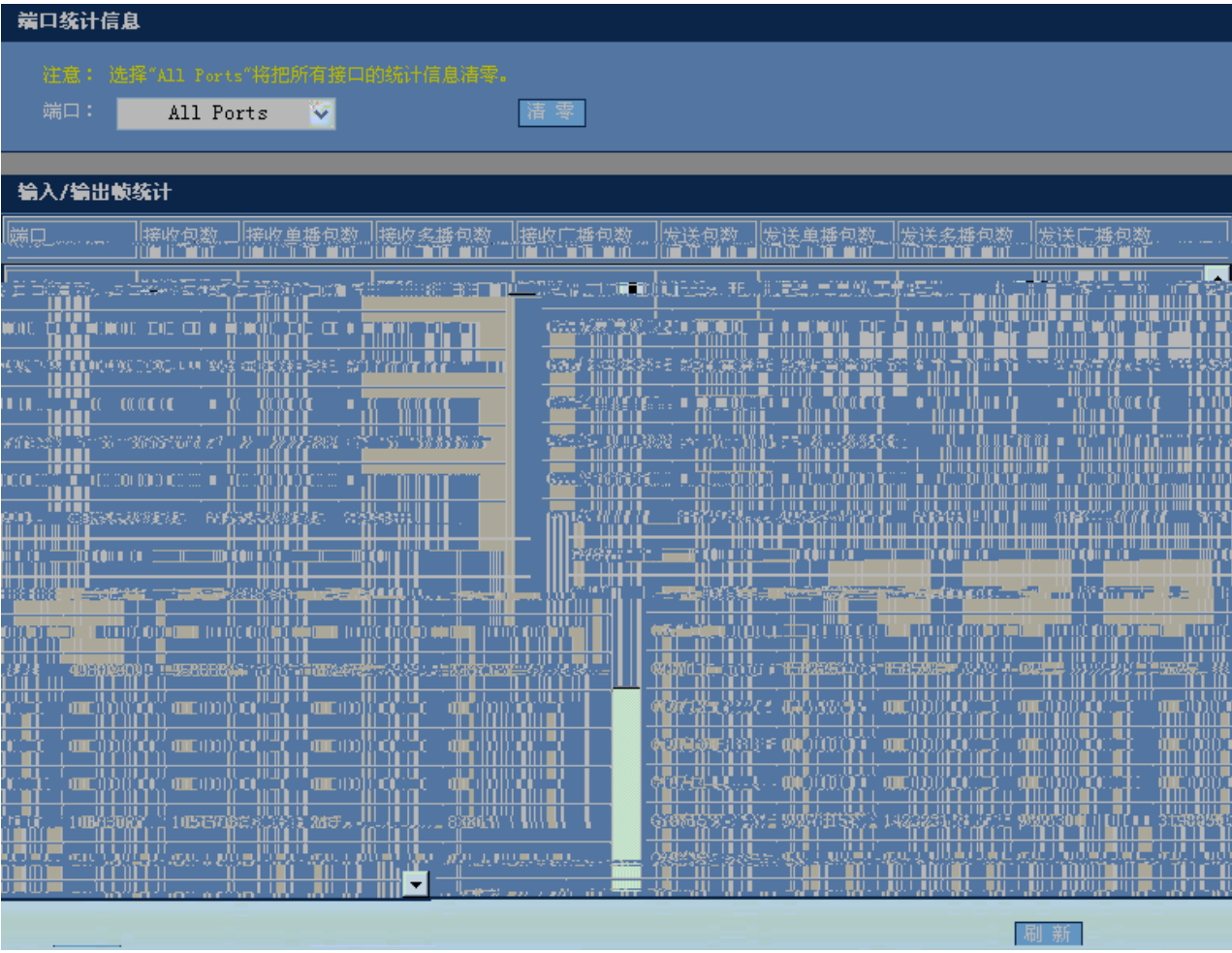
5-4 ʹ

端口运行状态	
端 口	带宽占用
FastEthernet 0/1	0%
FastEthernet 0/2	0%
FastEthernet 0/3	0%
FastEthernet 0/4	0%
FastEthernet 0/5	0%
FastEthernet 0/6	0%
FastEthernet 0/7	0%
FastEthernet 0/8	0%
FastEthernet 0/9	0%
FastEthernet 0/10	0%

、 ƒ ʹ ʹ E ʒ ʔ Ā

ʹ ʹ

5-5 ʹ ʹ



、 Γ a E^G π $\hat{A}$

a 、

5-6 a

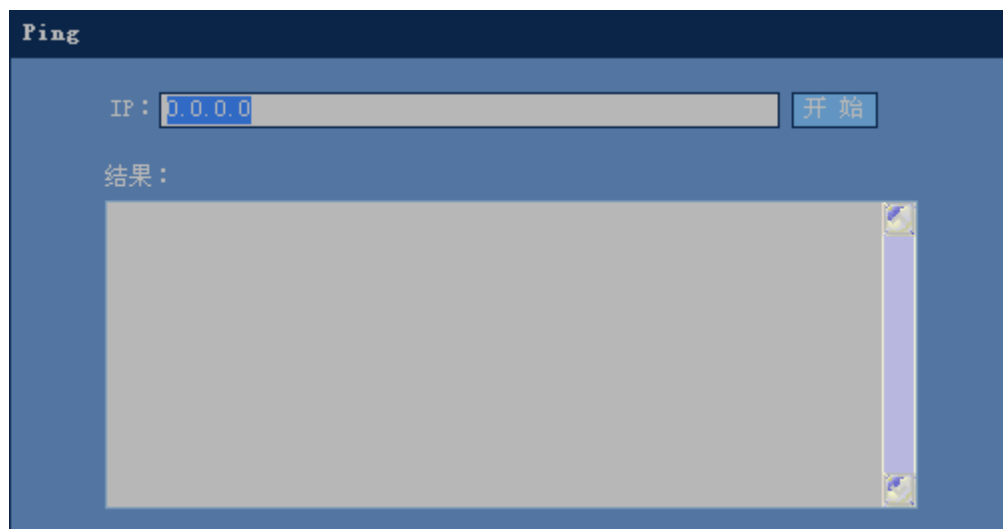
系统日志信息

```
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.
```

、 Ping 的 图 标

Ping

6-1 Ping

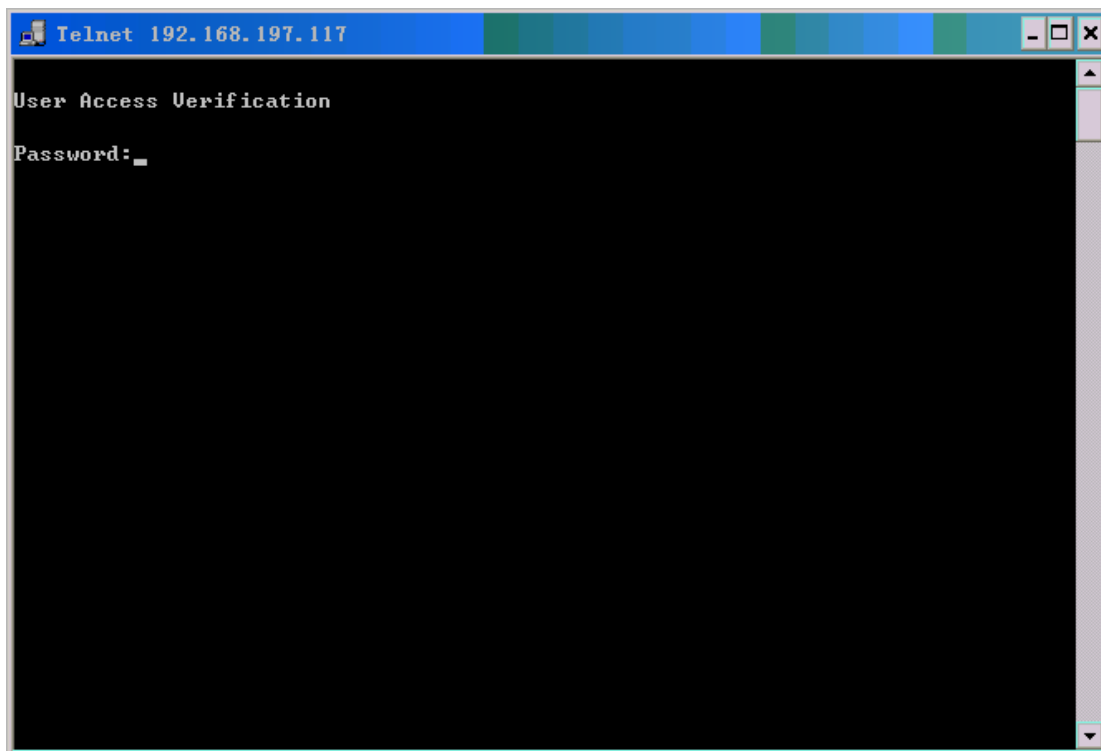


è 的 IP 地址 的 Ping 图标

、 Telnet 的 图 标

Telnet

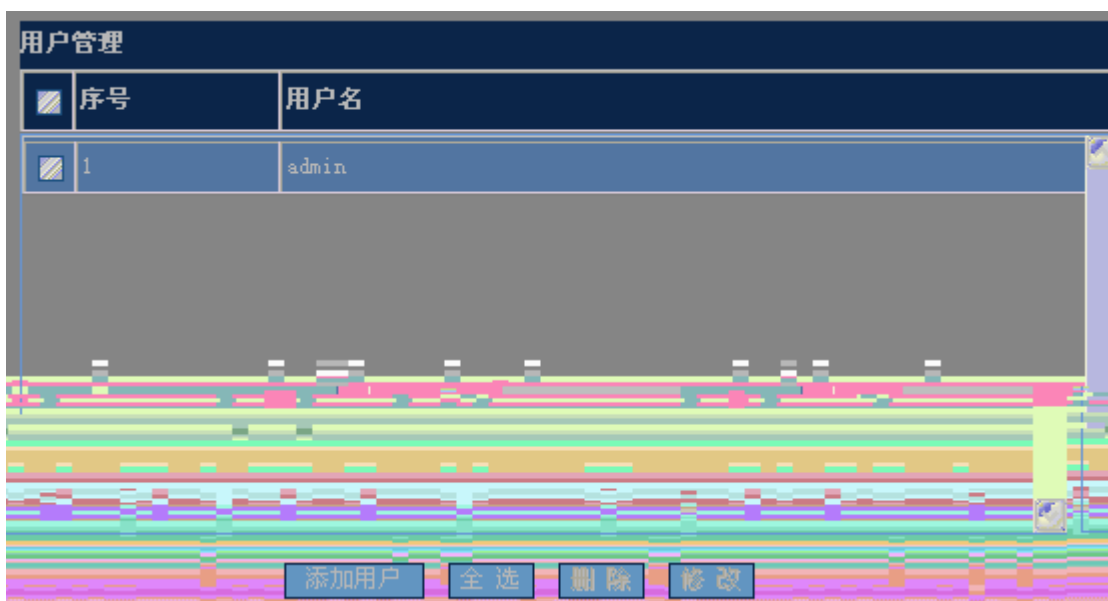
6-2 Telnet



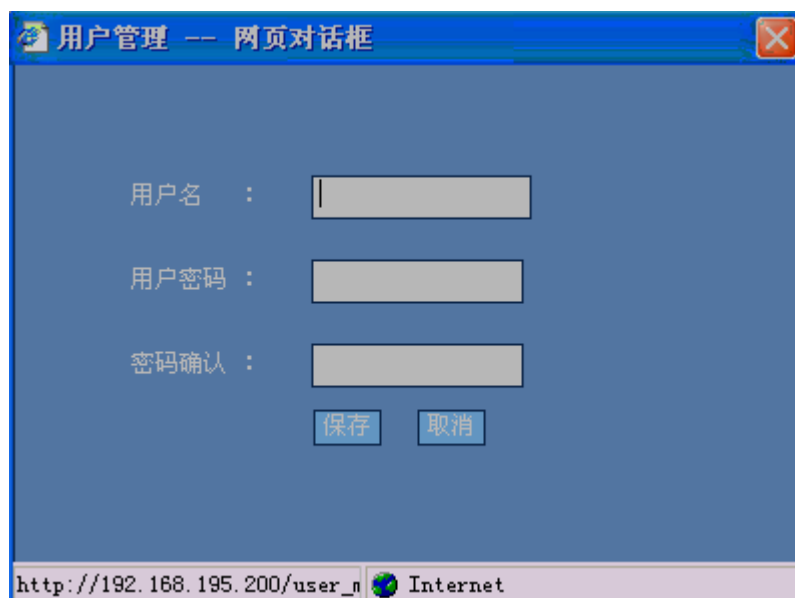
在 Telnet 窗口中，输入 Telnet 用户名，按 PC 键，输入 Telnet 密码，按 PC 键，按 PC 键。

在 Telnet 窗口中，输入 Telnet 用户名，按 PC 键，按 PC 键。

6-3

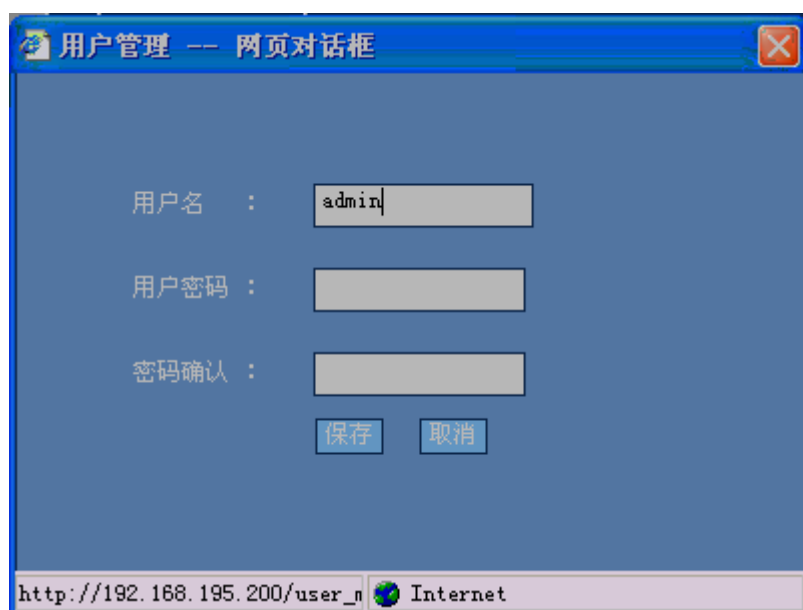


单击“用户管理”按钮，弹出“用户管理”对话框。



在“用户管理”对话框中，输入用户名“admin”，密码“123456”，并单击“保存”按钮。

6-5



单击“保存”按钮，弹出“用户管理”对话框。



、 P E G 卅 Â

6-6

修改Enable口令

注意：如果您设置了新的Enable口令，则在设置之后使用新口令重新登录。

新口令：

确认新口令：

保存

修改Telnet登录口令

新口令：

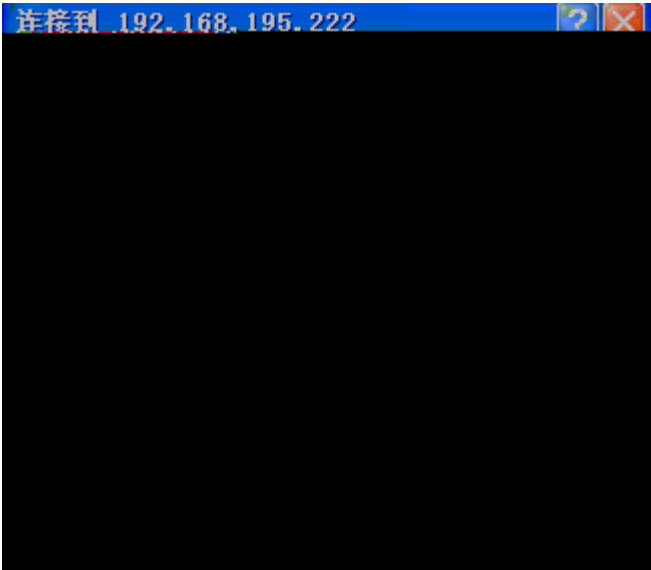
确认新口令：

保存

9 Enable 夗 3

9 Enable 夗 3 ǒ 夗 3 ± P ǒ E ǒ G Â

6-7



√ 3 Â

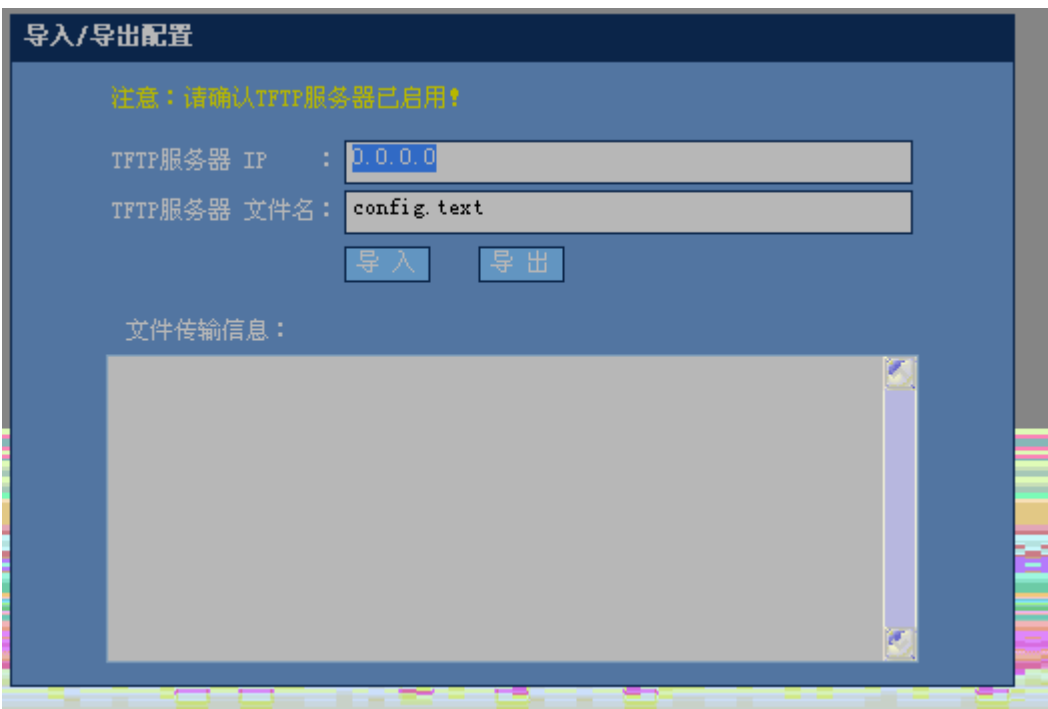
9 Telnet √ 3

9 Telnet √ 3 ò √ 3 ± Γ d L ~ G Â

、 Γ ò/ L G π Â

ò/ 、

6-8 ò/



单击“保存”按钮，保存配置。单击“使用默认端口”按钮，使用默认端口。

单击“使用默认端口”按钮，使用默认端口。

单击“使用默认端口”按钮，使用默认端口。

单击“使用默认端口”按钮，使用默认端口。

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)

单击“使用默认端口”按钮，使用默认端口。

单击“使用默认端口”按钮，使用默认端口。

单击“使用默认端口”按钮，使用默认端口。

