

WEB

RG-S5750-@

RGOS 10.4(2b12)p1

V1.0



RGOS®

RGNOS®



锐捷®

■

■

■

■

■

■

-
-
-

1.

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

2.



3.

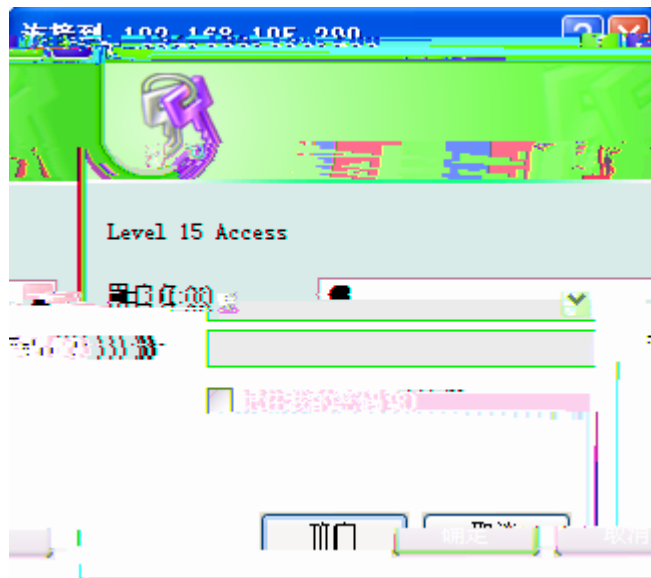
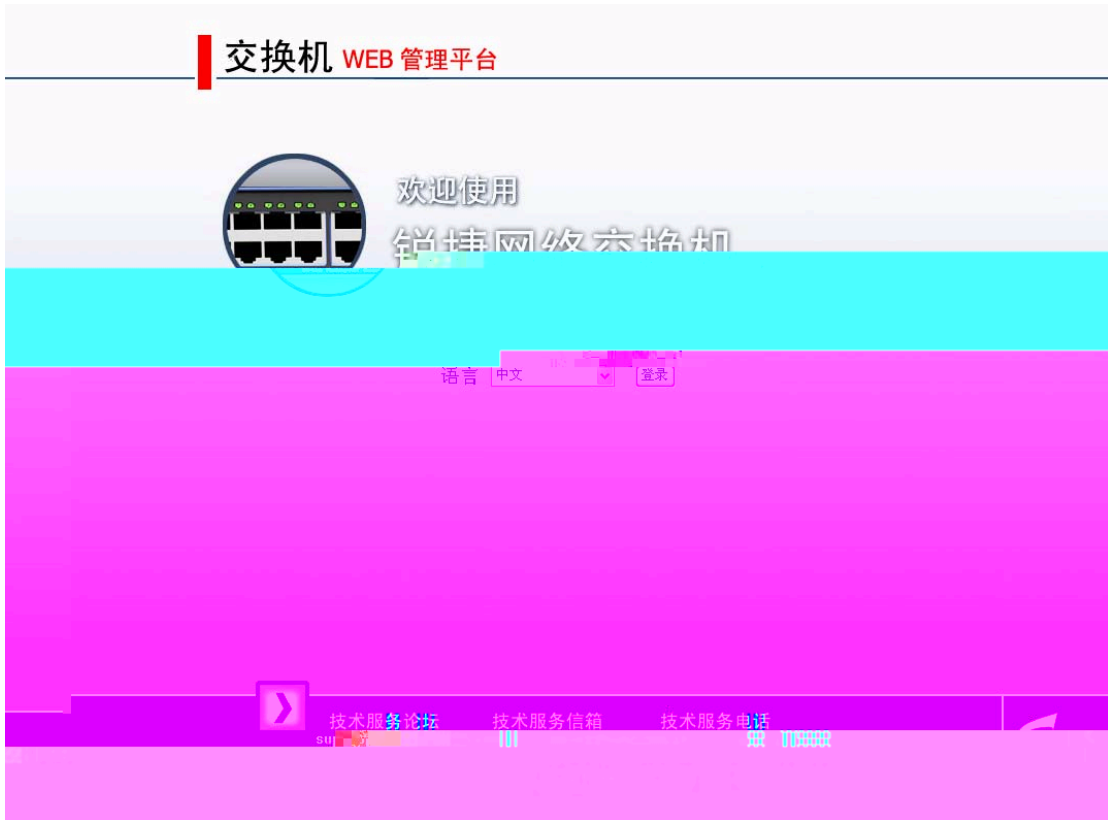
■

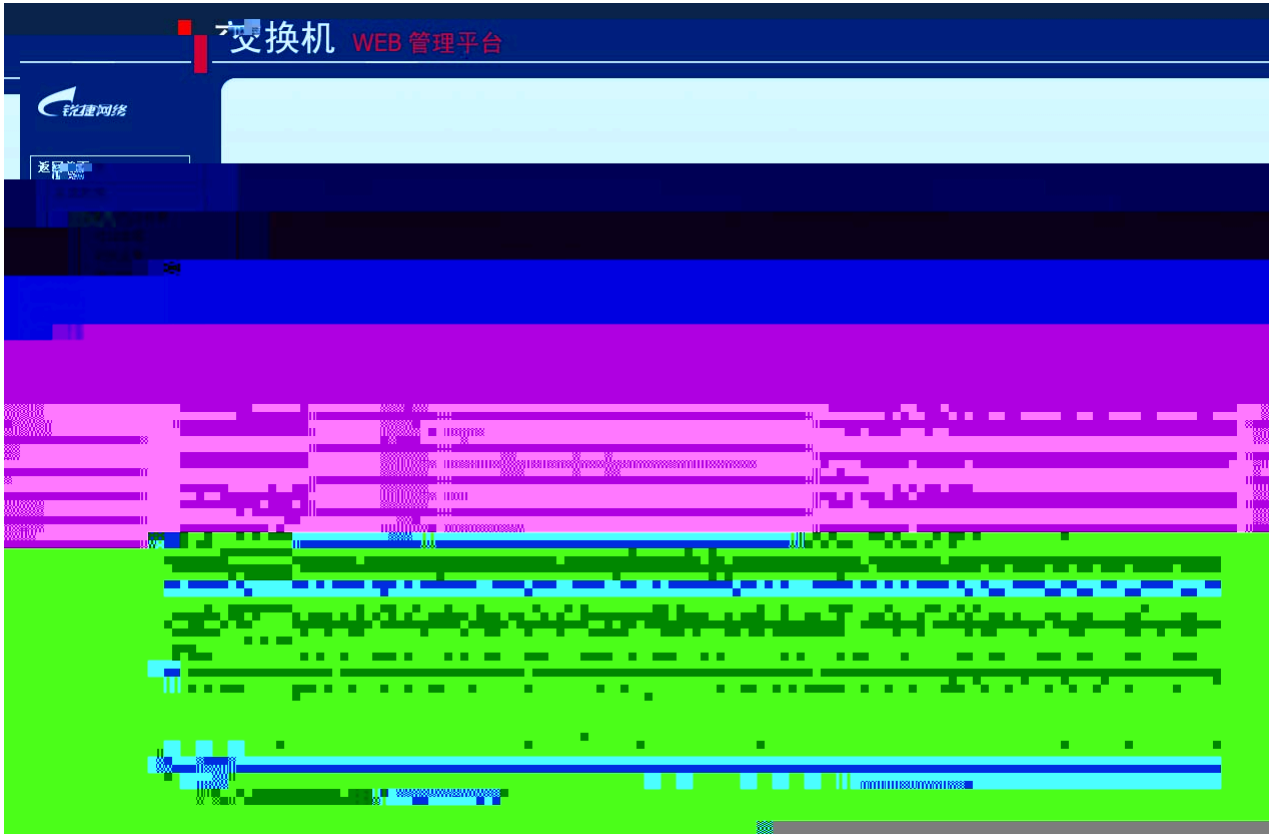
■

■



1 WEB





2.2

2.2.1 IP



2.2.2 VLAN

Local Area Network) 的简称, 它是在一个物理网络上划分出来的逻辑网络, 实现同一VLAN下的用户可以进行二层通讯, 不同VLAN下的用户无法进行二层通讯。

说明: VLAN是虚拟局域网 (Virtual LAN) 的简称, 它是在一个物理网络上划分出来的逻辑网络, 实现同一VLAN下的用户可以进行二层通讯, 不同VLAN下的用户无法进行二层通讯。

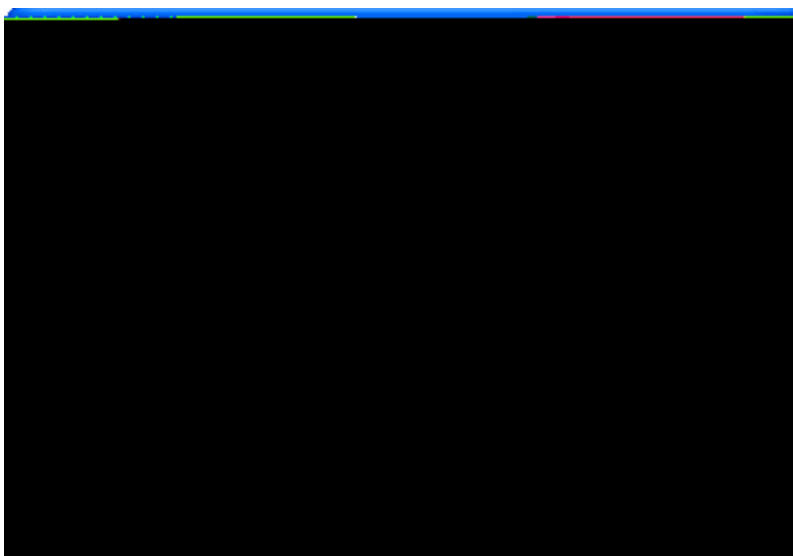
操作	VLAN ID	VLAN 名称
STATIC	<input type="checkbox"/> 1	VLAN0001
STATIC	<input type="checkbox"/> 2	VLAN0002

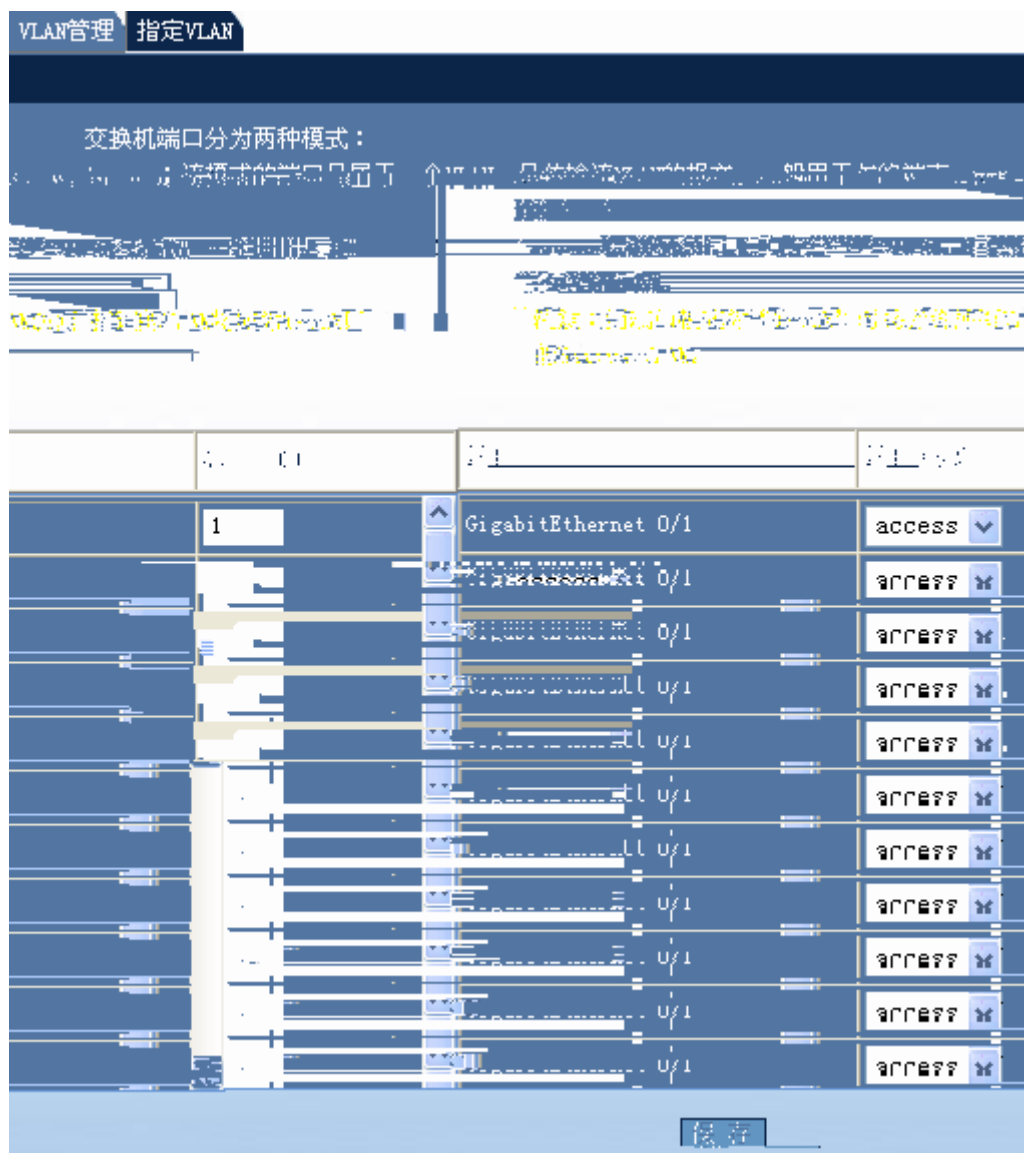
全选 删除 修改 新建

VLAN管理 -- 网页对话框

VLAN ID : (1-4094)

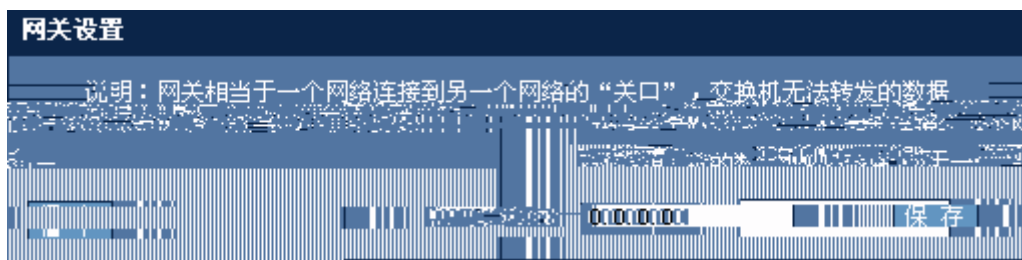
VLAN 名称 : (可选)





2.2.3

A'5`T,A' u- Ä



2.2.4



2.2.5

端口限速设置

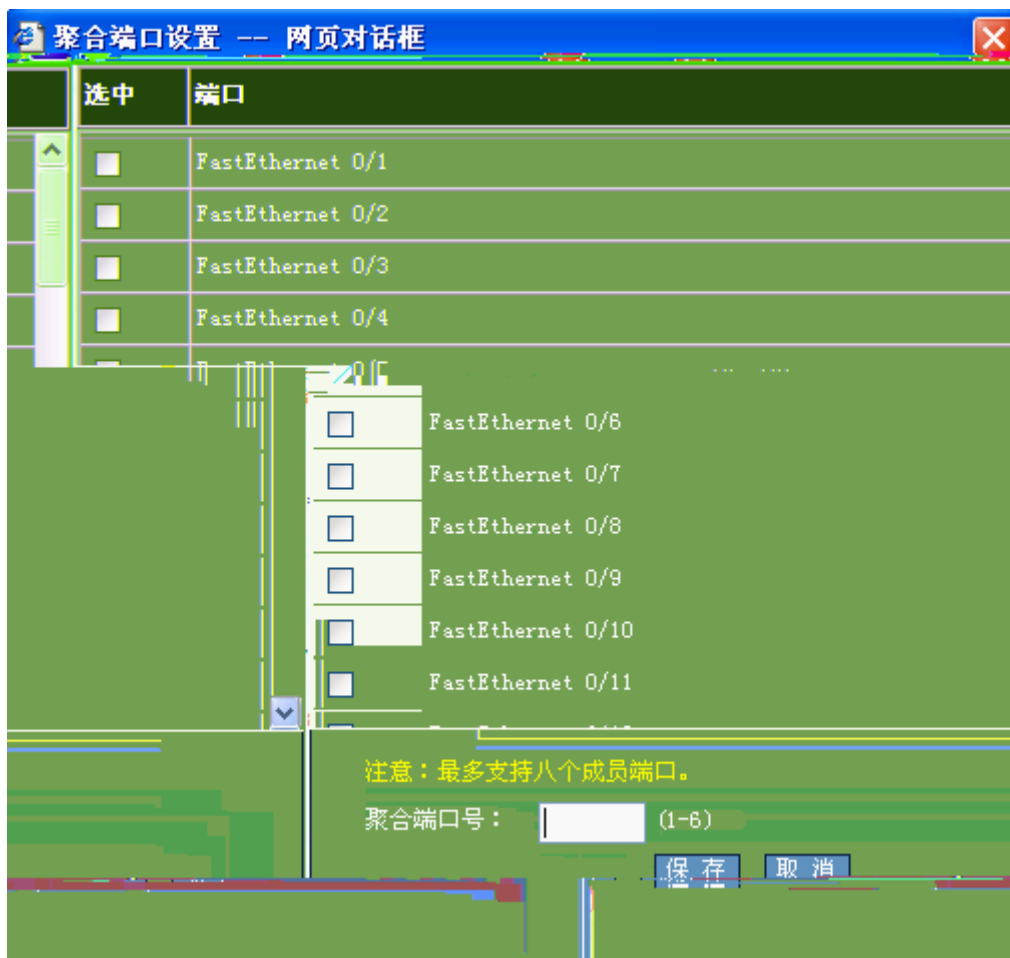
注意：不限速的端口，保持对应文本框为空（1byte=8bit）。S2900系列设备不支持对端口输入速率限制的设置。

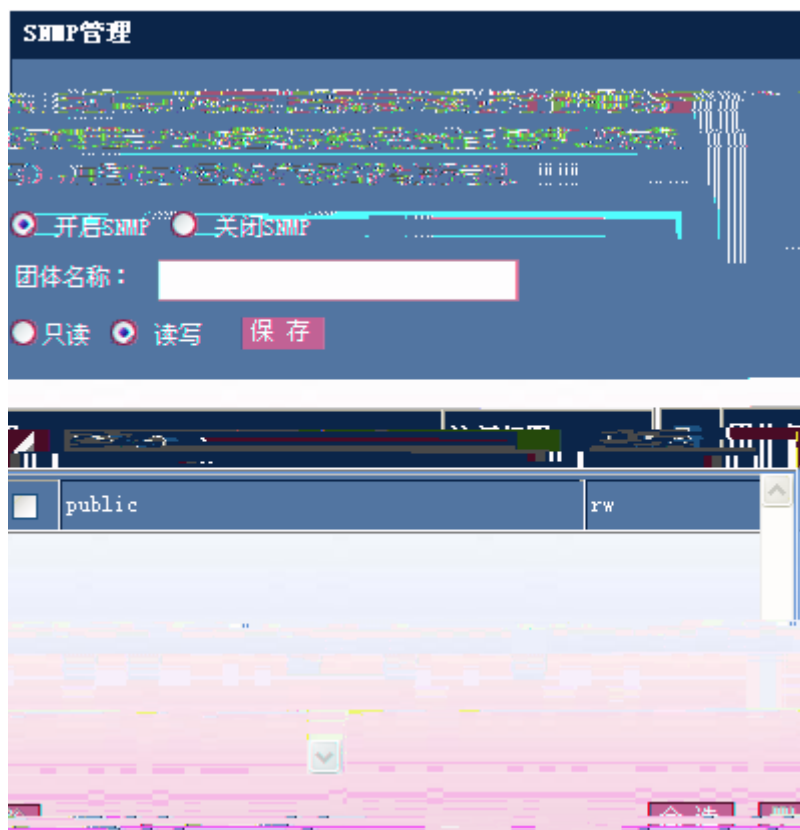
端口	输出速率限制 (312-1000000 KBit/s)	输入速率限制 (312-1000000 KBit/s)
GigabitEthernet 0/1	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/2	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/3	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/4	<input type="text"/>	<input type="text"/>
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"/>
GigabitEthernet 0/12	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/13	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/14	<input type="text"/>	<input type="text"/>
GigabitEthernet 0/15	<input type="text"/>	<input type="text"/>

保存 取消全部限速

2.2.6







2.2.12 NFPP

NFPP监控信息 NFPP配置 NFPP接口配置 NFPP日志

NFPP监控信息查看与配置

查看全部:

VLAN (1-4094) (可选) 端口 (可选) MAC (可选)

查看全部:

ARP扫描表信息					
	WLAN	interface	IP address	MAC address	timestamp
	1	Fa0/40	-	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 11:11:2
	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
			Fa0/40	001a.a942.f27f	2016-6-6 11:17:13
					2016-6-6 11:19:15
				Fa0/40	001a.a942.f27f 2016-6-6 11:21:26
				Fa0/40	001a.a942.f27f 2016-6-6 11:23:25
				Fa0/40	001a.a942.f27f 2016-6-6 11:24:26

配置管理 配置接口配置 配置日志

MFPP监控信息查看与配置

ARP 抗攻击配置 ICMP 抗攻击配置 DHCP 抗攻击配置 DHCPv6 抗攻击配置

IP地址: 192.168.0.110 子网掩码: 255.255.255.0

信任主机:

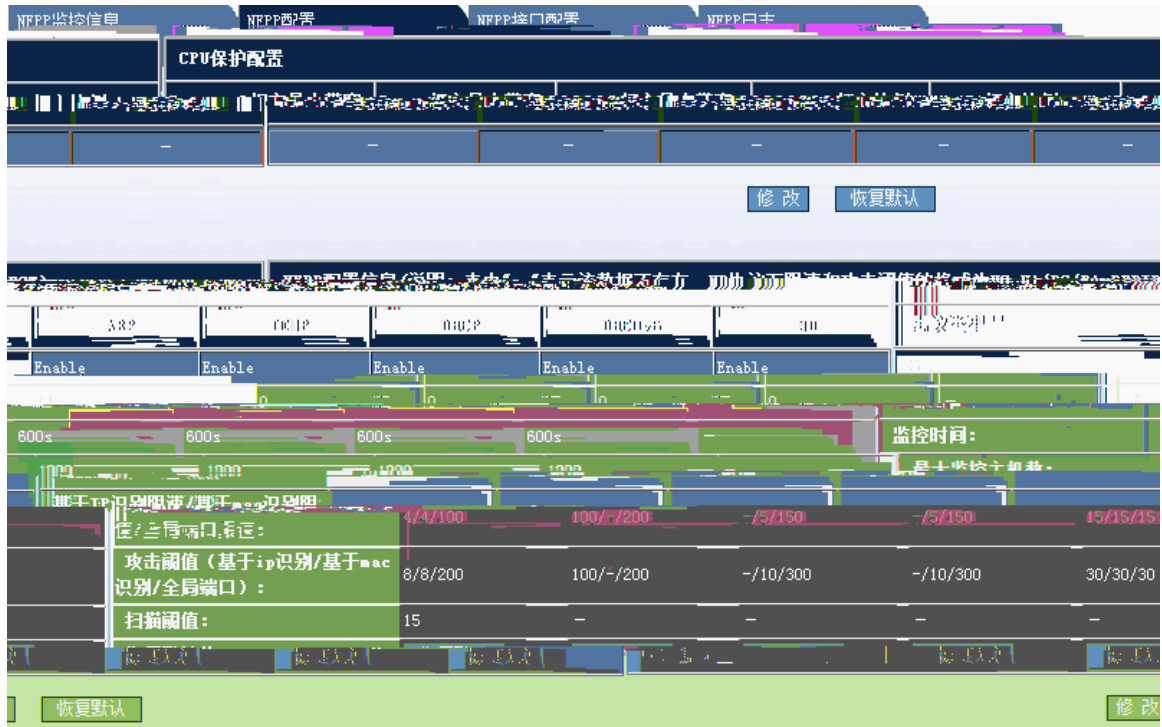
受监控主机信息

(ICMP)

不监控可信主机列表

IP地址	子网掩码
<input type="checkbox"/> 192.168.0.0	255.255.255.0

●



●



●

NFPP监控信息
NFPP配置
NFPP接口配置
NFPP日志

NFPP接口信息配置

● ICMP抗攻击配置
● DHCP抗攻击配置
● DHCPv6抗攻击配置
● DD抗攻击配置
● ARP抗攻击配置

0/1 开启ARP抗攻击 关闭ARP抗攻击 默认

(可选): 限速值: (1-9999) 攻击阈值: (1-9999)

(可选): 限速值: (1-9999) 攻击阈值: (1-9999)

(可选): 限速值: (1-9999) 攻击阈值: (1-9999)

(0/30-86400) (可选) 永久隔离 扫描阈值: (1-9999) (可选)

接口:

基于ip/vid/端口识别主机

基于mac/vid/端口识别主机

基于port端口识别主机 (可

隔离时间:

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)	扫描阈值	<input type="checkbox"/>	接口	ARP抗攻
	123	123/789/123	123/789/456	123	<input type="checkbox"/>	Fa0/1	Enable



MPPP接口信息配置

关闭ICMP抗攻击 默认 接口: **FastEthernet 0/1** 开启ICMP抗攻击

攻击阈值: (1-9999) 基于ip/vid/端口识别主机 (可选): 限速值: (1-9999)

攻击阈值: (1-9999) 基于port端口识别主机 (可选): 限速值: (1-9999)

隔离时间: (0/30-86400) (可选) 永久隔离

RT	攻击阈值 (基于IP/MAC/PORT)	接口	ICMP抗攻击状态	隔离时间	限速值 (基于IP/MAC/PORT)
	1222/-/2222	<input checked="" type="checkbox"/> Fa0/1	Enable	Permanent	1112/-/1322

●

NFPP监控信息 NFPP配置 **NFPP接口配置** NFPP日志

NFPP接口信息配置

接口: GigabitEthernet 0/1

值: 8888 (1-9999)	攻击阈值: 9999 (1-9999)	基于mac/vid/端口识别主机(可选): 限速
值: 8888 (1-9999)	攻击阈值: 9999 (1-9999)	基于port端口识别主机(可选): 限速

保存

-/8888/8888	-/9999/9999	Gi0/1	Enable	Permanent
-------------	-------------	-------	--------	-----------

全选 删除



NFPP监控信息 NFPP配置 **NFPP接口配置** NFPP日志

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攻击 关闭DHCPv6攻击

基于mac/vid/端口识别主机(可选): 限速值: 8888 (1-9999) 攻击阈值: 9999 (1-9999)

基于port端口识别主机(可选): 限速值: 8888 (1-9999) 攻击阈值: 9999 (1-9999)

隔离时间: Permanent (0/30-86400)(可选) 永久隔离

MAC/PORT	接口	DHCPv6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)
	<input type="checkbox"/> Gi0/1	Enable	Permanent	-/8888/8888	-/9999/9999

—

●

NFPP监控信息 NFPP配置 **NFPP接口配置** NFPP日志

NFPP接口信息配置

ARP 抗攻击配置 ICMP 抗攻击配置 DHCP 抗攻击配置 DHCPv6 抗攻击配置 DD 抗攻击配置

接口: 名称: 显示: 配置: 清除: 帮助:

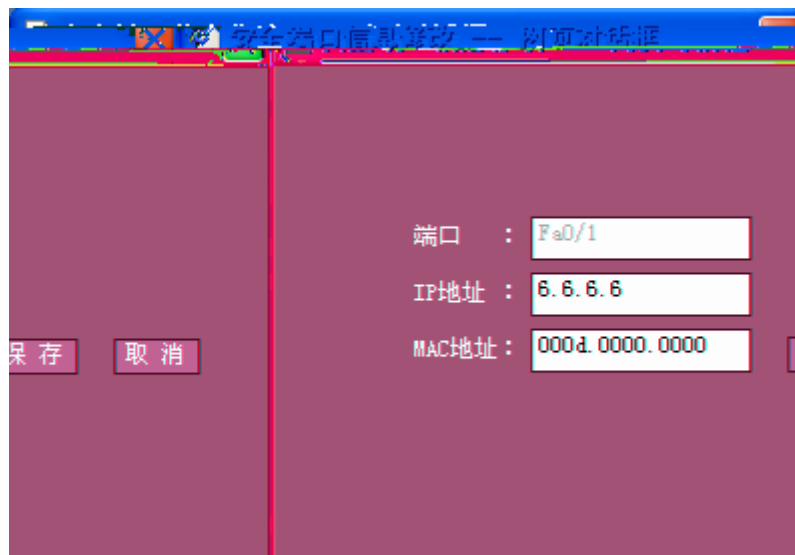
限速值: (1-9999) 攻击阈值: (1-9999) NS-NA模式:

限速值: (1-9999) 攻击阈值: (1-9999) 基于arp+seq id/端口 识别主机(勾选): 攻击模式:

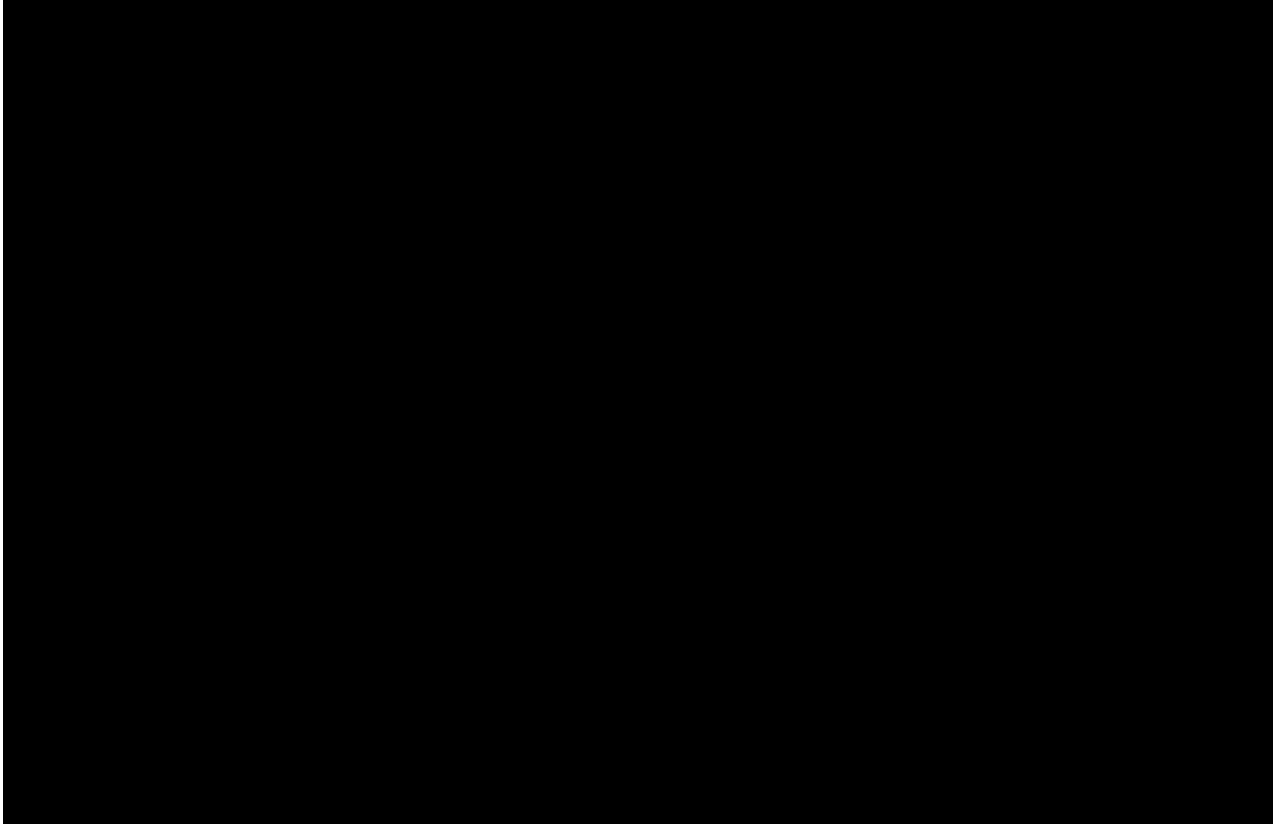
接口	状态	限速值	攻击阈值
<input checked="" type="checkbox"/> Gi0/1	Enable	8888/1111/3333	9999/2222/5555

WEB





2.3.4 ACL



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，功能将在DHCP Snooping控制范围内的接口上生效。

其他配置项：... 保存 ...

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
<input type="checkbox"/> FastEthernet 0/6	ip	active	deny-all	-	-
<input type="checkbox"/> FastEthernet 0/14	ip	active	deny-all	-	-

全选 删除



2.3.6 DAI

arp报文接收统计信息				
Slot	Type	Pps	Total	Drop
MainBoard	arp	10	324430	0

各类型报文的带宽和优先级配置状态				
Type	Pos	Pri		
arp-guard	180	7		
arp	180	7		
dot1x	2000	4		
lldp	180	7		
erps	180	7		
erps	180	7		
erps	180	7		
tunnel-bpdu	180	6		
ipv4-icmp-local	1600	6		
lldp	180	5		
lldp_cdp	180	5		
cfm-pdu	180	3		

管理板/单机/堆叠系统的接收报文的统计信息				
Type	Pps	Total	Drop	
arp	10	324430	0	
arp-guard	180	7		
dot1x	2000	4		
erps	180	7		
erps	180	7		
erps	180	7		
tunnel-bpdu	180	6		
ipv4-icmp-local	1600	6		
lldp	180	5		
lldp_cdp	180	5		
cfm-pdu	180	3		

2.3.9 RADIUS

The screenshot shows a web interface for configuring RADIUS servers. It is divided into several sections:

- AAA参数配置 (AAA Parameter Configuration):**
 - AAA new-model: 开启 关闭
 - 密钥: 隐藏密钥 [input field] [保存]
 - 记帐计费更新功能: 开启 关闭
 - 非连续认证服务器动态: [input field] [保存]
 - IP授权模式: [input field] suppli
- RADIUS服务器配置 (RADIUS Server Configuration):**
 - RADIUS服务器IP地址: 192.168.0.111
 - UDP认证端口: [input field] (0-65535)
 - UDP记账端口: [input field] (0-65535)
 - [保存]
- RADIUS服务器列表 (RADIUS Server List):**

认证端口	记账端口	服务器状态	RADIUS服务器IP地址
1812			192.168.0.111
			1813

[全选] [删除]

AAA参数配置

AAA new-model

计费: 开启 关闭 记帐计费更新功能

非锐捷认证服务器: 开启 关闭 非锐捷认证服务器

IP授权模式: enable disable 保存

Radius服务器组

组名:

Radius服务器IP地址:

UDP认证端口: (0-65536) (可选)

UDP记账端口: (0-65536) (可选)

保存

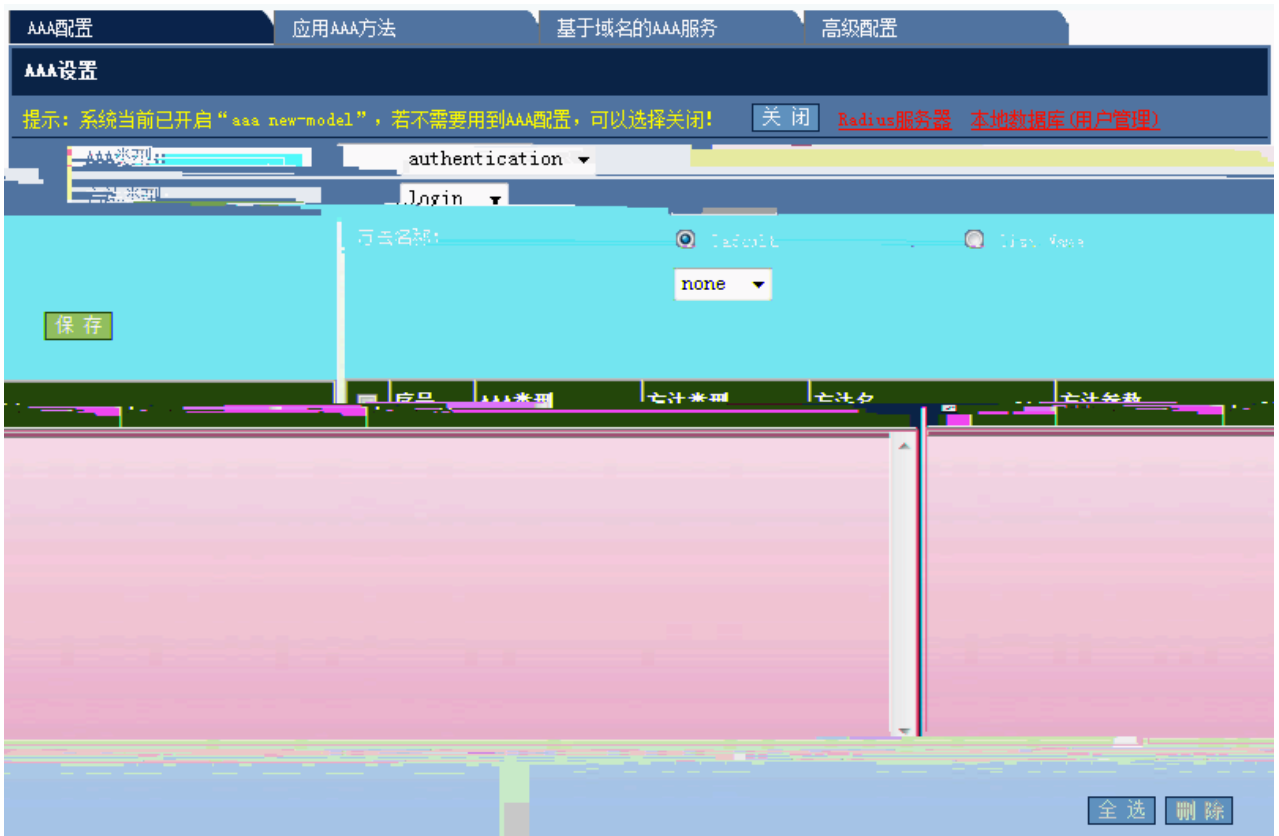
管理: 删除 刷新

Terminal Output:

```

radius group radius=====
radius server 1
  authentication
  accounting
  state active
  server 1
  authentication
  accounting
  state active
radius server 2
  authentication
  accounting
  state active
radius server 3
  authentication
  accounting
  state active
  
```

2.3.10 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

域名: Default: Domain Name

认证方法: default ▾

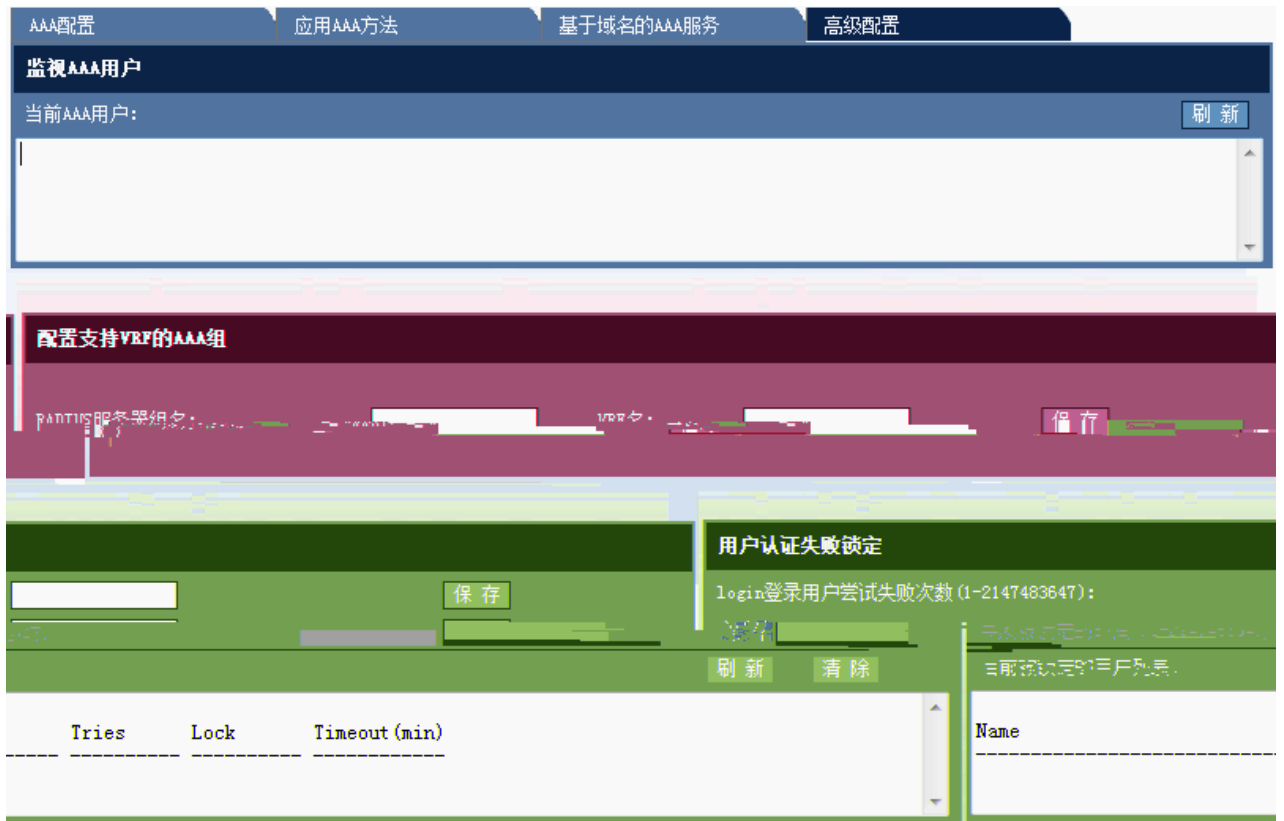
授权方法: default ▾

记账方法 (network): default ▾

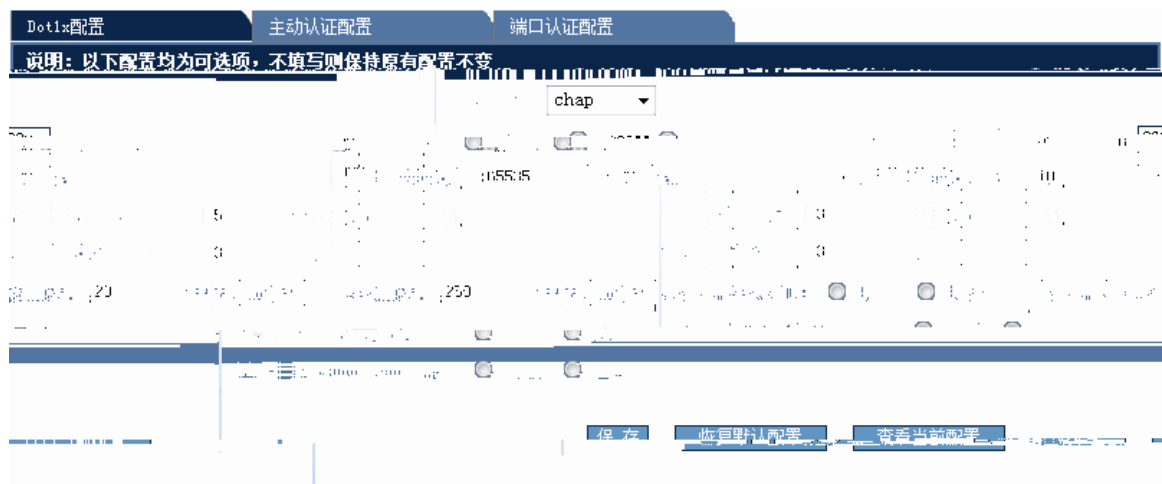
with domain without domain

AAA Domain管理: ▾

```
=====  
State: Block  
Username format: With-domain  
Access limit: 2  
802.1X Access statistic: 0  
  
Selected method list:  
authentication dot1x default  
authentication ppp default  
authorization network default
```



2.3.11 Dot1x





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: 查询

MAC地址: 绑定

序号	IP	MAC
----	----	-----

全选 删除 刷新

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

2.3.13 WEB

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

应用于端口

端口: IP Only Mode

<input type="checkbox"/>	序号	端口	IP Only Mode
<input type="checkbox"/>	1	FastEthernet 0/1	YES
<input type="checkbox"/>	2	FastEthernet 0/3	YES

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

2.3.14 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。

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

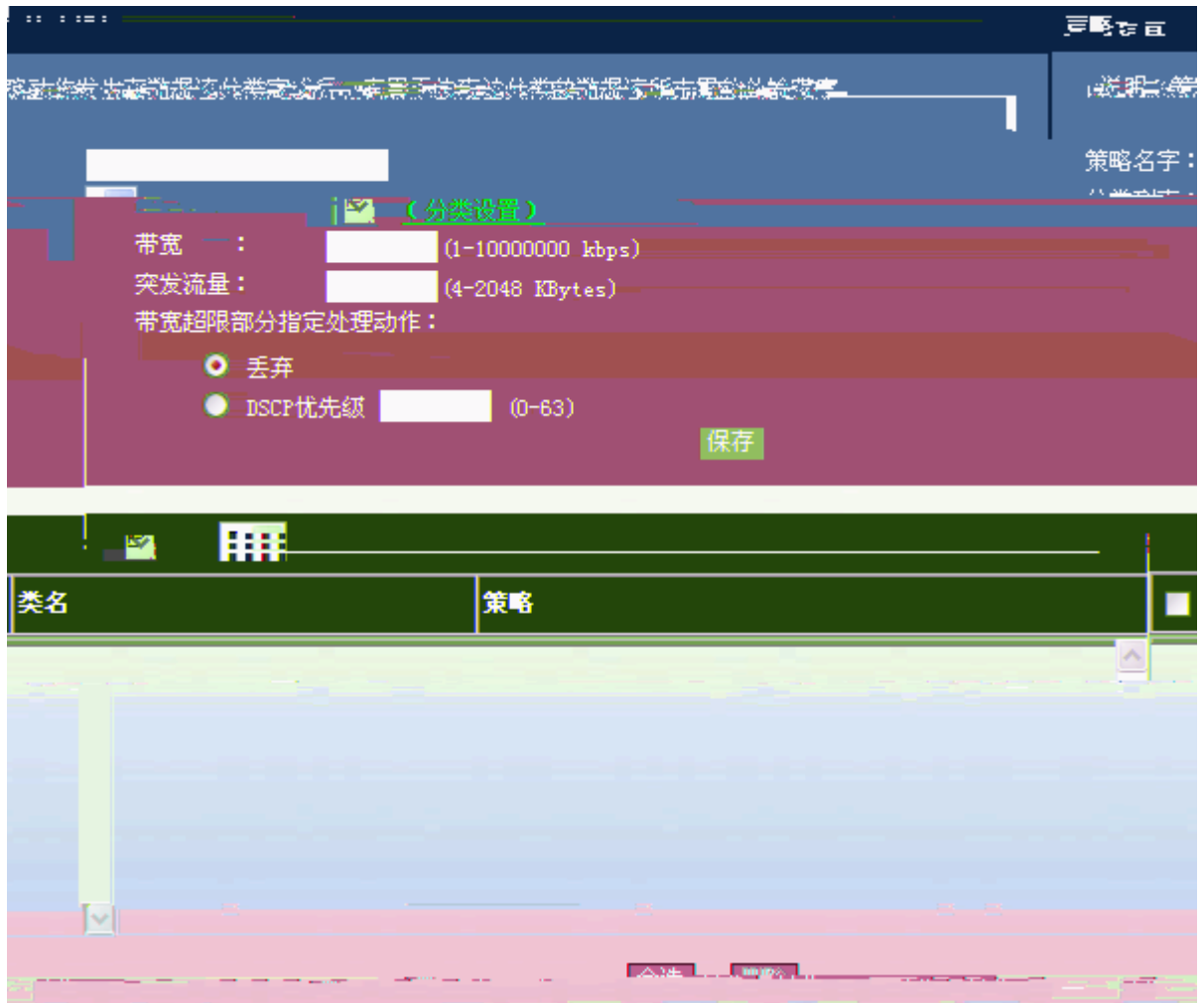
DHCP Snooping 信任端口设置

端口：

DHCP Snooping配置信息

■	端口	信任端口

限速



2.4.3

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： ▼

策略列表： [\(策略设置\)](#)

限速方向：
 输入限速
 输出限速

<input type="checkbox"/>	端口	方向	策略名	信任模式	COS
<input type="checkbox"/>	FastEthernet 0/1	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/2	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/3	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/4	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/5	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/6	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/7	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/8	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/9	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/10	-	-	-	-
<input type="checkbox"/>	FastEthernet 0/11	-	-	-	-

2.4.4

基本配置 安全地址 安全地址绑定

安全地址的最大个数(0~100,可输入) 安全地址的老化时间(0~1440分钟,可输入)

静态(静态的时间同时适用于手工配置的安全地址和自动学习的地址) 启用Sticky MAC地址学习功能

处理违例方式: restrict restrict restrict

保存

	安全地址的最大个数	老化时间	static	启用Sticky MAC地址学习功能	处理违例方式	接口
	-	-	-	-	restrict	<input type="checkbox"/> FastEthernet 0/4
	100	1	YES	YES	restrict	<input type="checkbox"/> FastEthernet 0/5

全选 删除

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 type="checkbox"/>	FastEthernet 0/1	1000.0000.0000	10	1.2.3.3

2.5

2.5.1

系统信息	
设备型号：	S2924G
主机名：	Ruijie
软件版本：	RGOS (Ruijie) Release 10.2.00(3) (3035F23195A44470348C)
操作系统：	Linux
MAC地址：	001E1010B041

2.5.2

当前配置

```
Building configuration...
Current configuration : 12931 bytes

!
version RGNOS 10.2.00(3), Release(3035F23195A44470348C)
!
!
!
!
vlan 1
 name vlan1
!
vlan 2
!
vlan 3
!
vlan 4
!
vlan 5
!
vlan 6
!
vlan 7
!
```

5) (Tue Mar 11 19:23:04 2008 -

2.5.3

端口状态					
端口	状态	Vlan	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

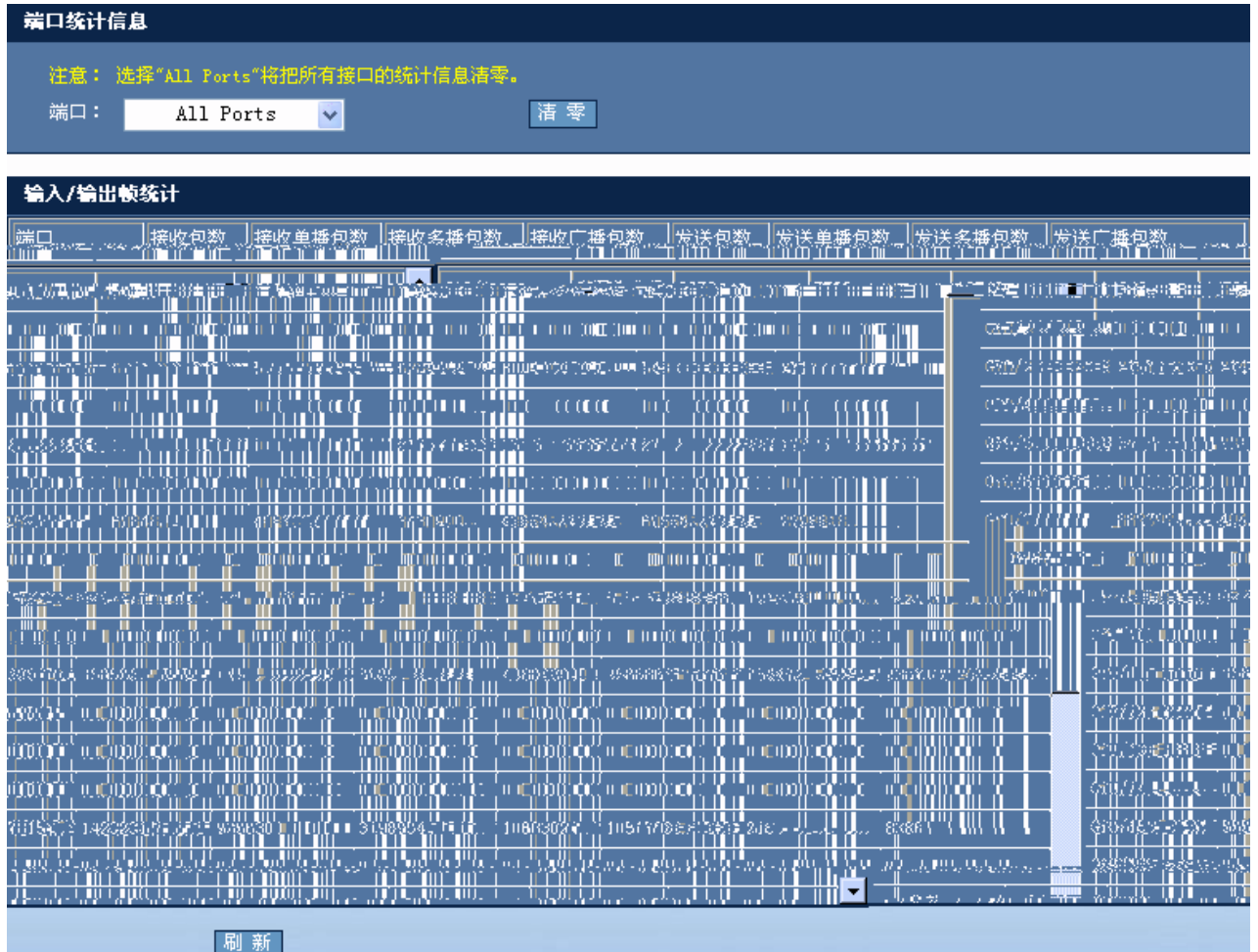
刷新

2.5.4

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%

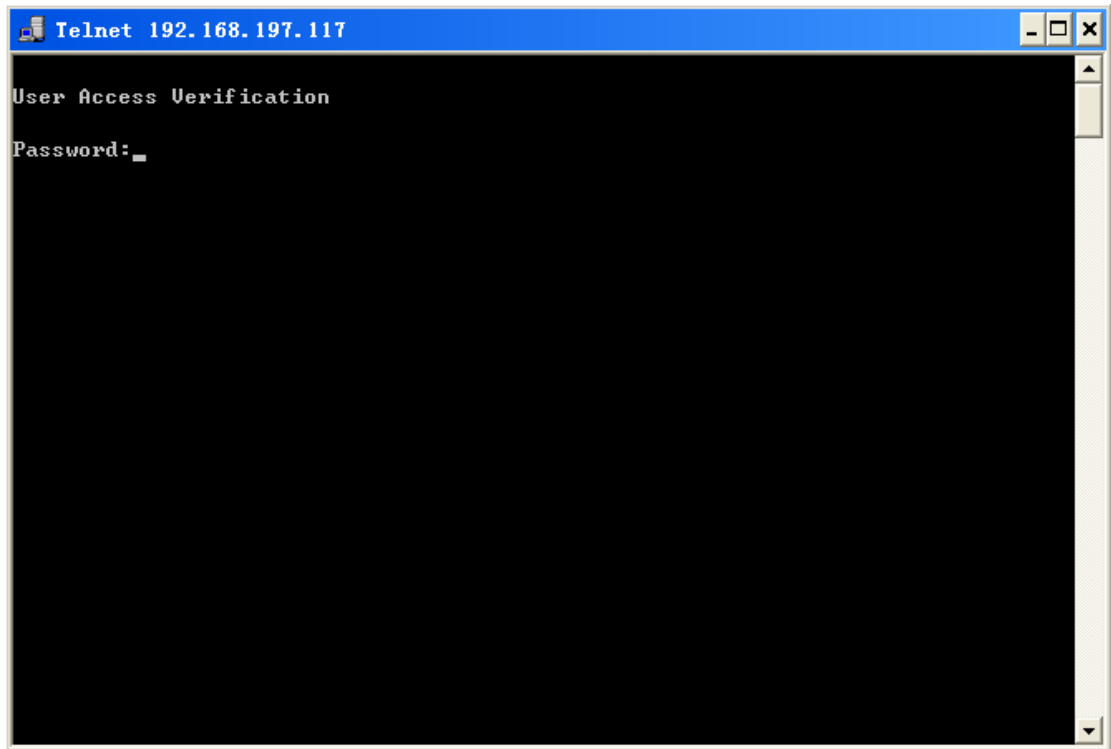
刷新

2.5.5

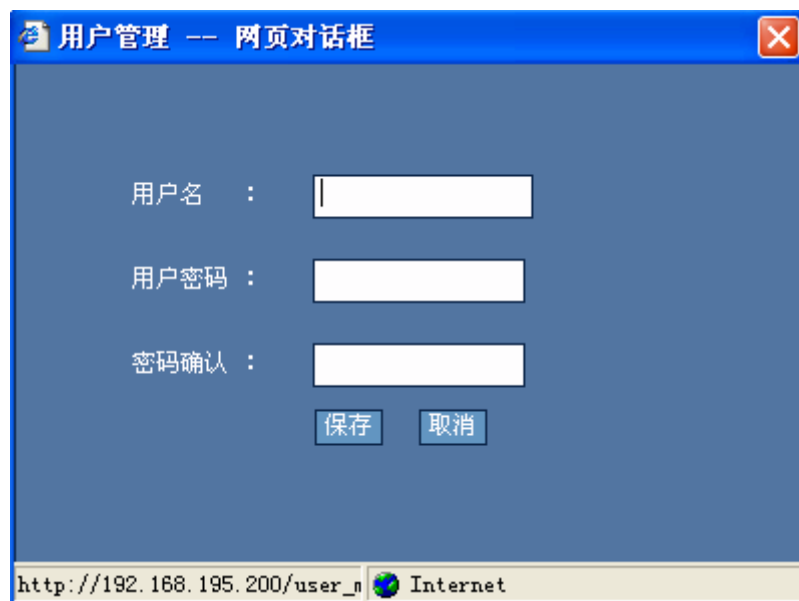


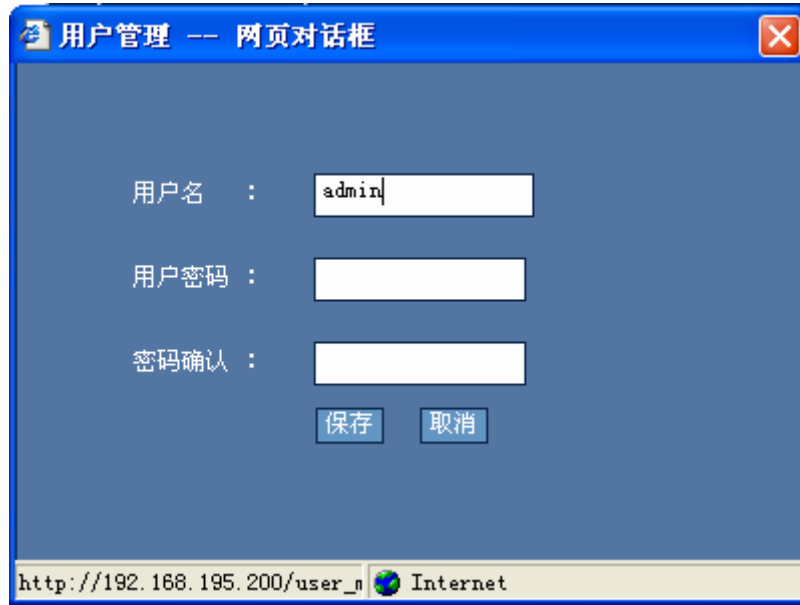
2.5.6

2.6.2 Telnet



2.6.3





2.6.4

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



2.6.5 /

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：

2.6.6 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)

2.8 WEB

2.8.1

2.8.2

2.8.3

2.8.4

```
Ruijie#configure
```

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

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

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

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

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

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

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

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

Ruijie(config)#enable service web-server

Ruijie(config)#ip http authentication enable

Ruijie(config)#enable password admin

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

2.8.5

```
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
username admin privilege 15
no service password-encryption
ip http authentication local

enable service web-server
!
....
.....
!
interface VLAN 1

ip address 192.168.100.1 255.255.255.0
no shutdown
```

```
!  
!  
line con 0  
line vty 0 4  
  login  
!  
!  
end
```

```
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  
enable service web-server  
!  
....  
.....  
!  
interface VLAN 1  
  
  ip address 192.168.100.1 255.255.255.0  
  
  no shutdown  
!  
!  
line con 0  
line vty 0 4  
  login  
!  
!  
end
```
