ZHE ヽ Ᵽ ừ Q

UJ0V9333 ヿ ̃ ƥ ̓O ū

UJRV 4317+6e49,s5

ή ” ○ ˝ M σ Y213

○ Ű ɵ ΫǪ

ƒ Â

a ЛЬ ƒ à à à à à

è à è ƒ Â

 à  à  à  à

 à  à RGOS® à  à

 à  à  à 锐捷®

a Â

Ԁ ԉ ɵ ΫǪ

è è Â

Ю Â

è a

a Â

| ƍ

◌ ˝ ը Ѽ

ԻԱ ׀ ɾ

Ю

ẽ ŭ ạ ĭ

Â

Â

Â

× Ь

б ⅂

ȁ Ԋ⁄... ӈ

Ɨ ʒ Â

Â

a Â

ɻ Â

Ю

Ɨ ˚ a Â

Ɨ è ˆ à ˜ é Љ

Â

ʒ Ю Љ Ь Â

1 WEB

1.1 WEB

1.2

1.2.1

1.2.2

1.3 WEB

“ ”

1.4 WEB


Level 15 Access


交换机IP设置
注意：如果激活交换机的IP地址，请用新的IP地址重新登录WEB。
VLAN ID
IP地址
子网掩码
状 态
1
192.168.195.200
255.255.255.0
激活
2
192.168.1.2
255.255.255.0
修 改

“ ”


交换机IP设置 -- 网页对话框
注意：如果激活修改后的VLAN，请确保激活后的VLAN的IP
VLAN ID ：
2
IP地址 ：
192.168.1.2
子网掩码：
255.255.255.0
激活状态：
激活（UP）
未激活（DOWN）
保存
取消
Internet
http://192.168.195.200/ip_mod

“ ”

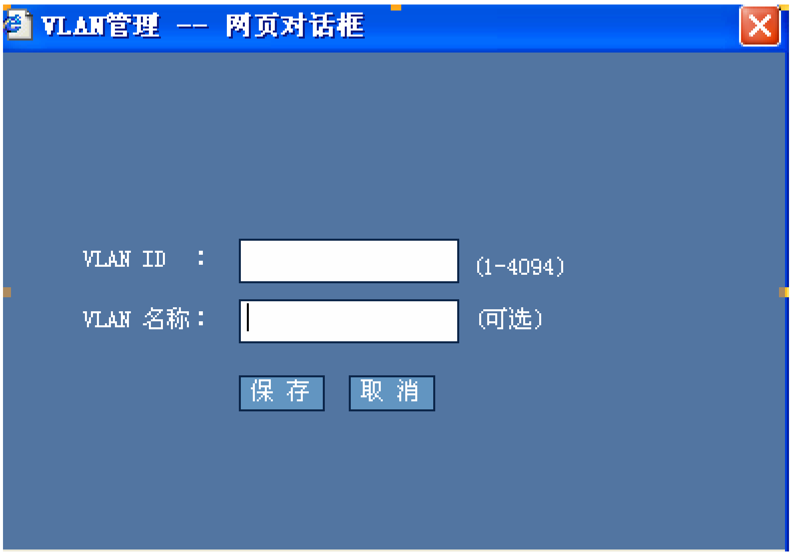
1.5.2 VLAN

“ ”


说明：VLAN是虚拟局域网（ Virtual L
下的用户无法进行二层通讯。
STATIC
STATIC
1
VLAN0001
2
VLAN0002
全 选
删 除
修 改
新 建

VLAN

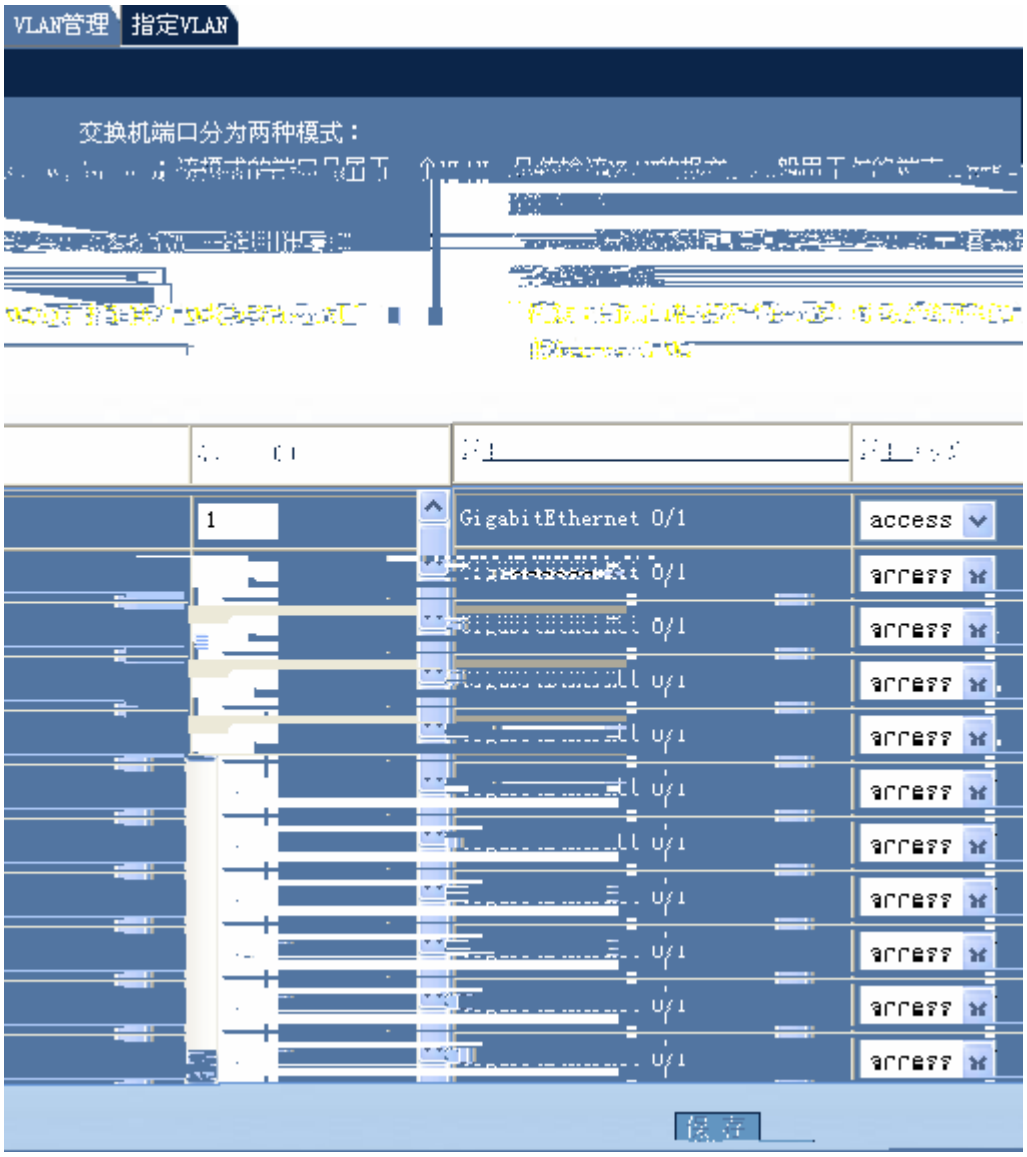
“ ”



“ ”

VLA ÈAĘEÃ(a);ÜlA,ó'SÁ(S@EB-g-Ð/$4@ÔL8p@ýJ, ßÀ!5BÞçÀ @

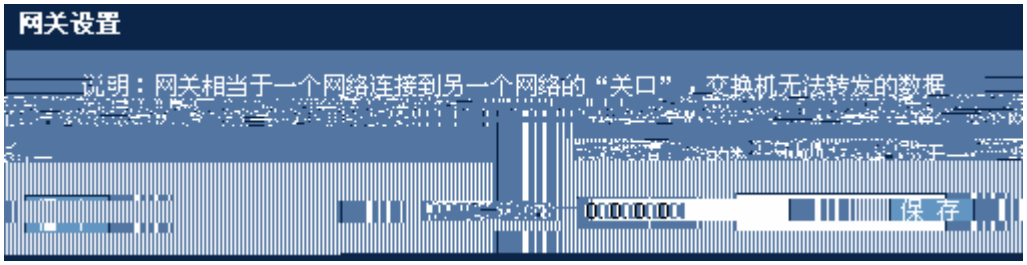
ô Ô ´Vps• 9 / $ 1 @ ðÀ *ó Ð¦



“ ”

1.5.3

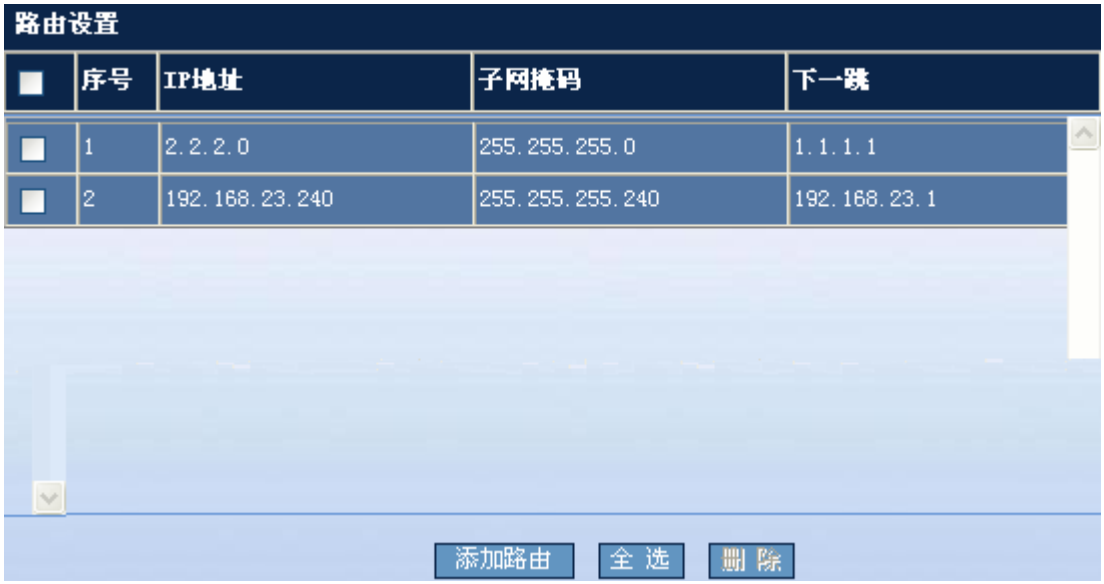
“ ”


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
保 存

“ ”

1.5.4

“ ”


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

“ ”

“ ”

“ ”

1.5.5

“ ”


端口镜像设置
注意：设置交换机的端口监控，监控端口与被监控端口不能是同一个端口。如果指定了同一端口，该端口将被配置成监控端口。
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
GigabitEthernet 0/13
GigabitEthernet 0/14
GigabitEthernet 0/15
GigabitEthernet 0/16
GigabitEthernet 0/17
GigabitEthernet 0/18
GigabitEthernet 0/19
GigabitEthernet 0/20
GigabitEthernet 0/21
GigabitEthernet 0/22
GigabitEthernet 0/23
GigabitEthernet 0/24
所有数据
删除端口监控
保 存

“ ”

“ ”

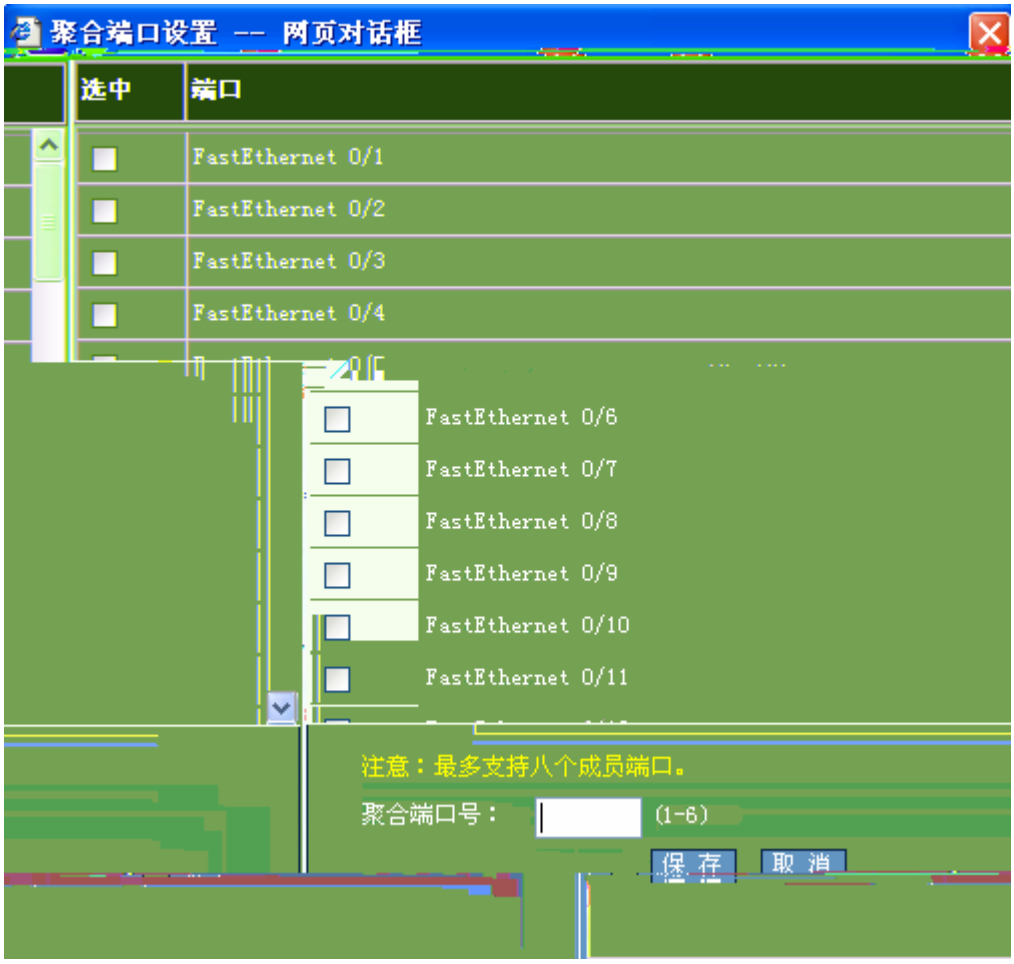
1.5.6

“ ”


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
瞬时速率限制
GigabitEthernet 0/4
GigabitEthernet 0/5
GigabitEthernet 0/7
GigabitEthernet 0/9
GigabitEthernet 0/10
GigabitEthernet 0/11
取消全部输入限速

“ ”

“ ”


聚合端口设置 -- 网页对话框
选中
端口
FastEthernet 0/1
FastEthernet 0/2
FastEthernet 0/3
FastEthernet 0/4
FastEthernet 0/6
FastEthernet 0/7
FastEthernet 0/8
FastEthernet 0/9
FastEthernet 0/10
FastEthernet 0/11
注意：最多支持八个成员端口。
聚合端口号：
(1-6)
保 存
取 消

“ ”

“ ”

1.5.8

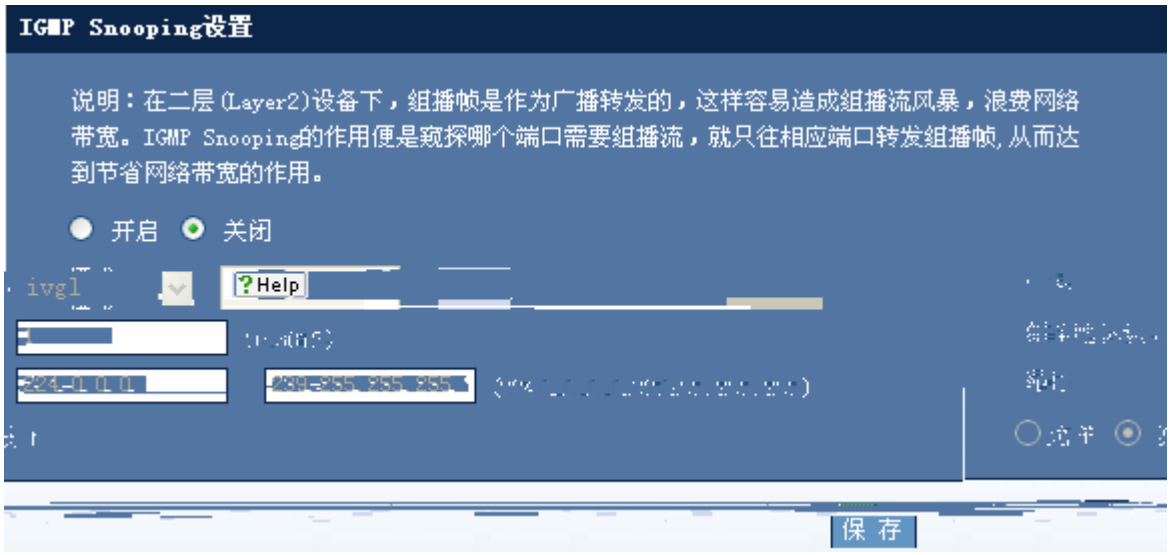
“ ”


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：
Up
双工：
Half
速率：
10
流控：
On
描述：
保 存
Gi0/1 Down Half 10 On -
Gi0/2 Down Half 10 On -
Gi0/3 Down Full 1000 Off -
Gi0/4 Down Auto Auto Off -
Gi0/5 Down Full 100 Off -
Gi0/6 Down Auto Auto Off -
Gi0/7 Up Full 100 Off -
Gi0/8 Down Auto Auto Off -
Gi0/9 Down Full 100 Off -
Gi0/10 Down Auto Auto Off -
刷 新

“ ”

1.5.9 DHCP

“ ”


IGMP Snooping设置
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
保 存

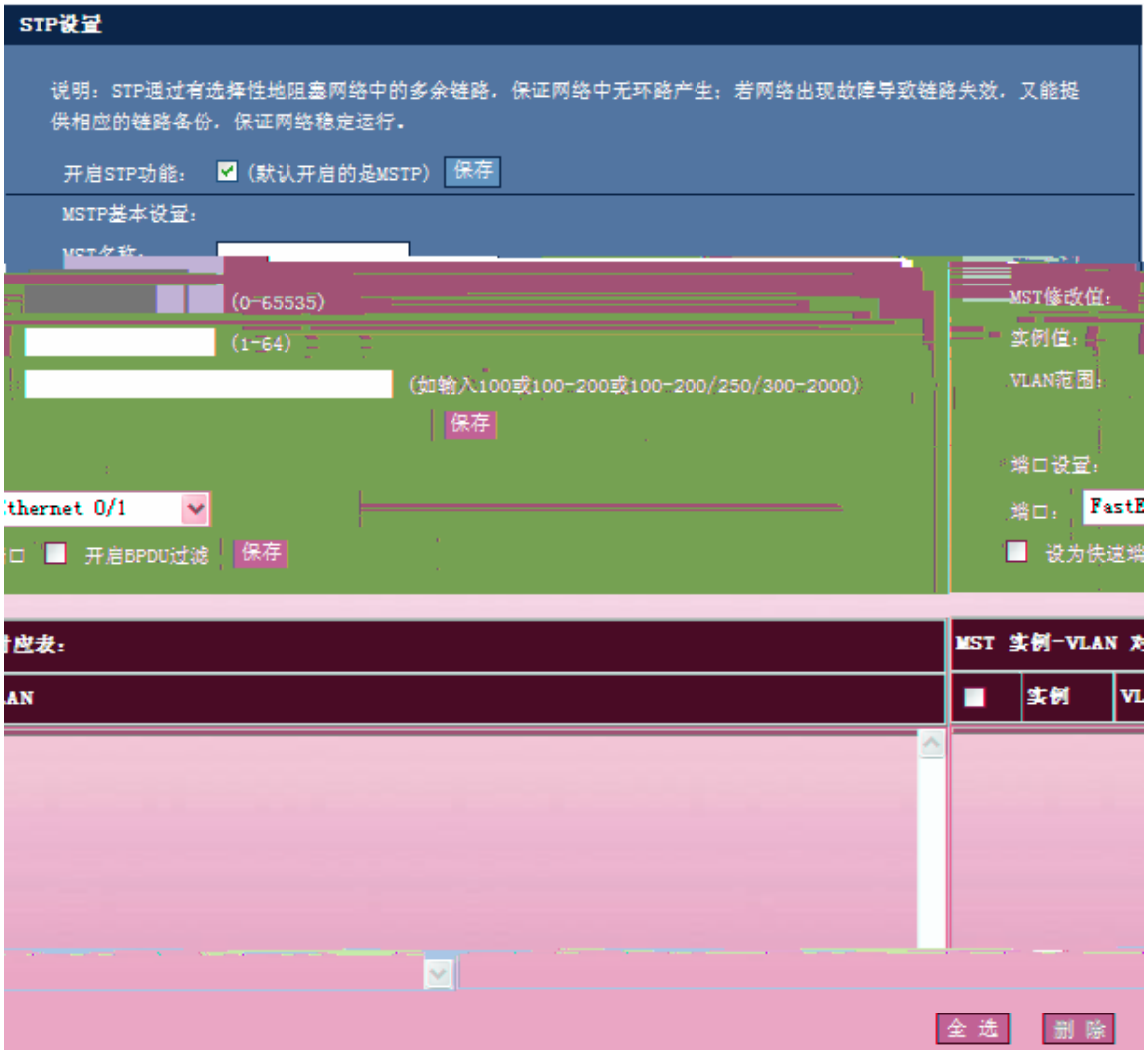
“ ”

“ ”

“ ” “ ”

1.5.11 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：
(0-65535)
(1-64)
(如输入100或100-200或100-200/250/300-2000)
保存
MST修改位：
实例值：
VLAN范围：
端口设置：
端口：
设为快速端
thernet 0/1
开启BPDU过滤
保存
MST 实例-VLAN
实例
全 选
删 除

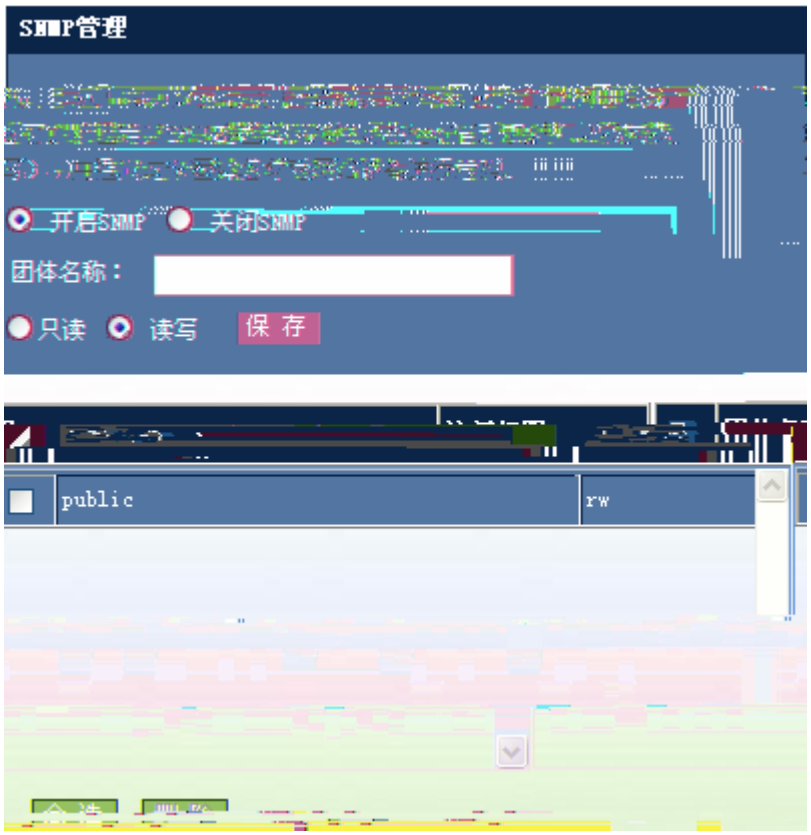
“ ” “ ”

“ ”

“ ”

1.5.12 SNMP

“ ”



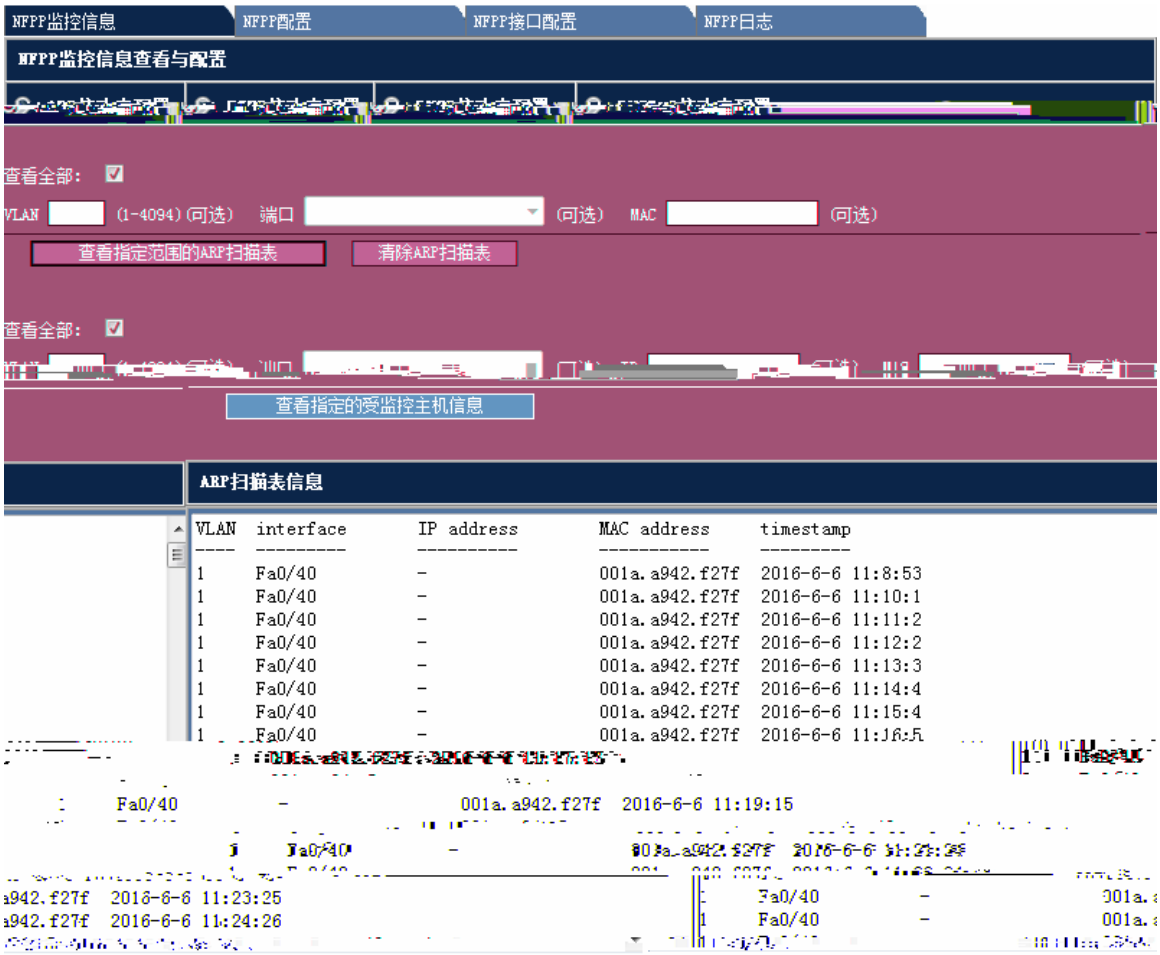
“ ”

“ ” “ ” “ ”

“ ”

1.5.13 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)
查看指定范围的ARP扫描表
清除ARP扫描表
查看全部:
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
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
Fa0/40 - 001a.a942.f27f 2016-6-6 11:19:15
a942.f27f 2016-6-6 11:23:25
a942.f27f 2016-6-6 11:24:26

“ ”

“ ”

“ ”


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
ARP抗攻击配置
ICMP抗攻击配置
DHCP抗攻击配置
DHCPv6抗攻击配置
查看全部：
VLAN
(1-4094)(可选)
端口
(可选)
MAC
(可选)
查看指定的受监控主机信息
受监控主机列表
全选
删除

“

”

“

”

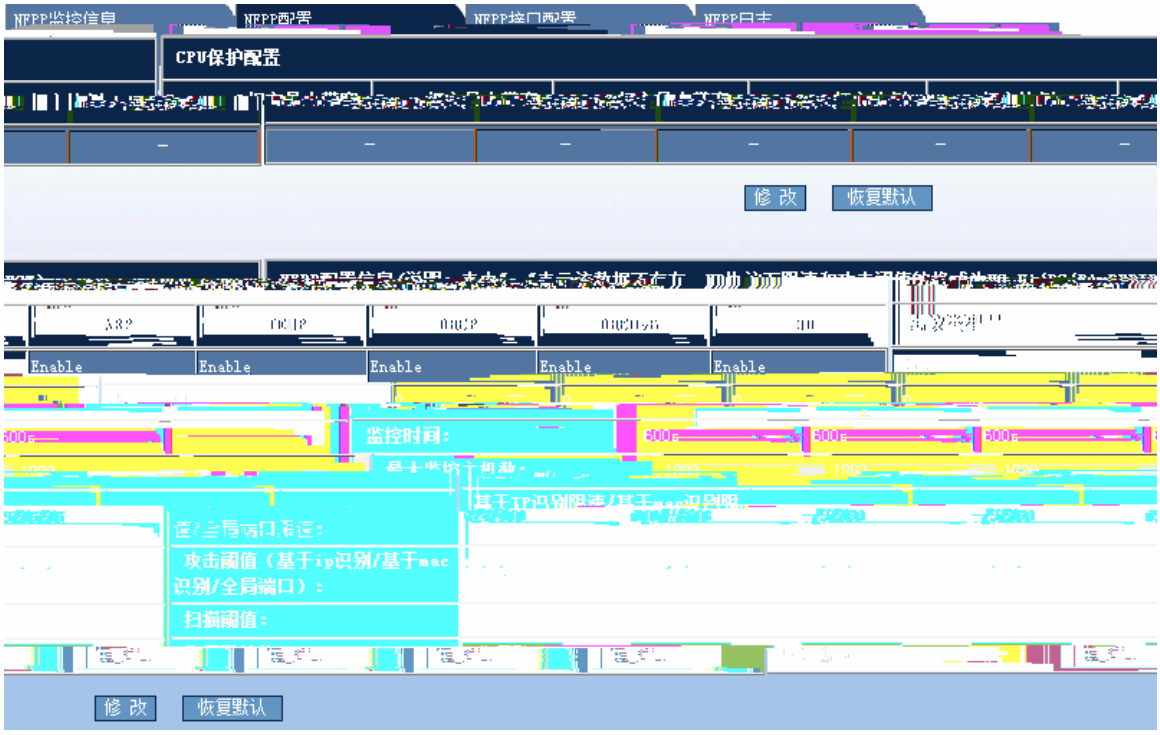
—


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
ARP抗攻击配置
ICMP抗攻击配置
DHCP抗攻击配置
DHCPv6抗攻击配置
查看全部：
VLAN
(1-4094)(可选)
端口
(可选)
MAC
(可选)
查看指定的受监控主机信息
受监控主机列表
VLAN
接口
受监控主机的mac地址
剩余监控时间
全选
删除

“

” “ ”

NFPP

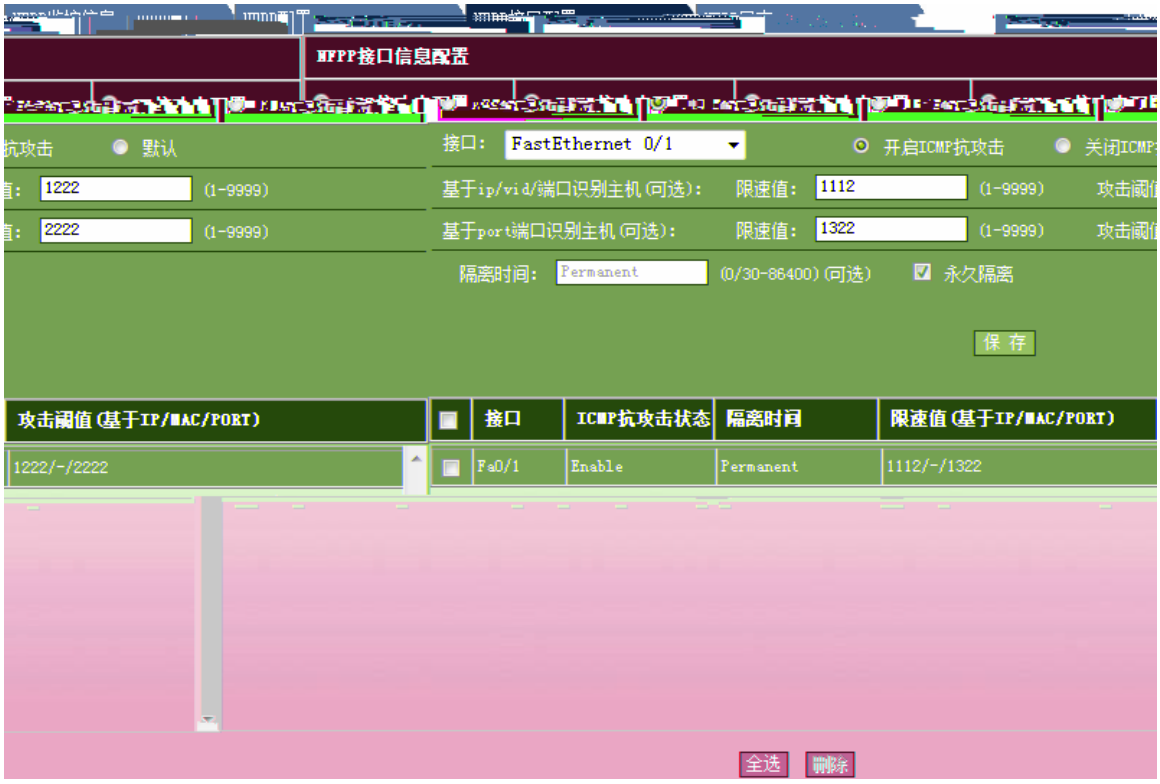

NFPP监控信息
NFPP配置
NFPP接口配置
NFPP日志
CPU保护配置
修 改
恢复默认
Enable
Enable
Enable
Enable
Enable
监控时间:
攻击阈值（基于ip识别/基于mac识别/全局端口）:
扫描阈值:
修 改
恢复默认


网页对话框
8000
(1-8192)(可选)
8000
(1-8192)(可选)
8000
(1-8192)(可选)
35
(1-98)(可选)
45
(1-98)(可选)
保 存
取 消


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
ND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
接口：
FastEthernet
(可选)：
限速值：
123
(1-9999)
攻击阈值：
123
(1-9999)
基于ip/vid/端口识别主机
(可选)：
限速值：
789
(1-9999)
攻击阈值：
789
(1-9999)
基于mac/vid/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抗攻
123
123/789/123
123/789/456
123
Fa0/1
Enable
全选
删除

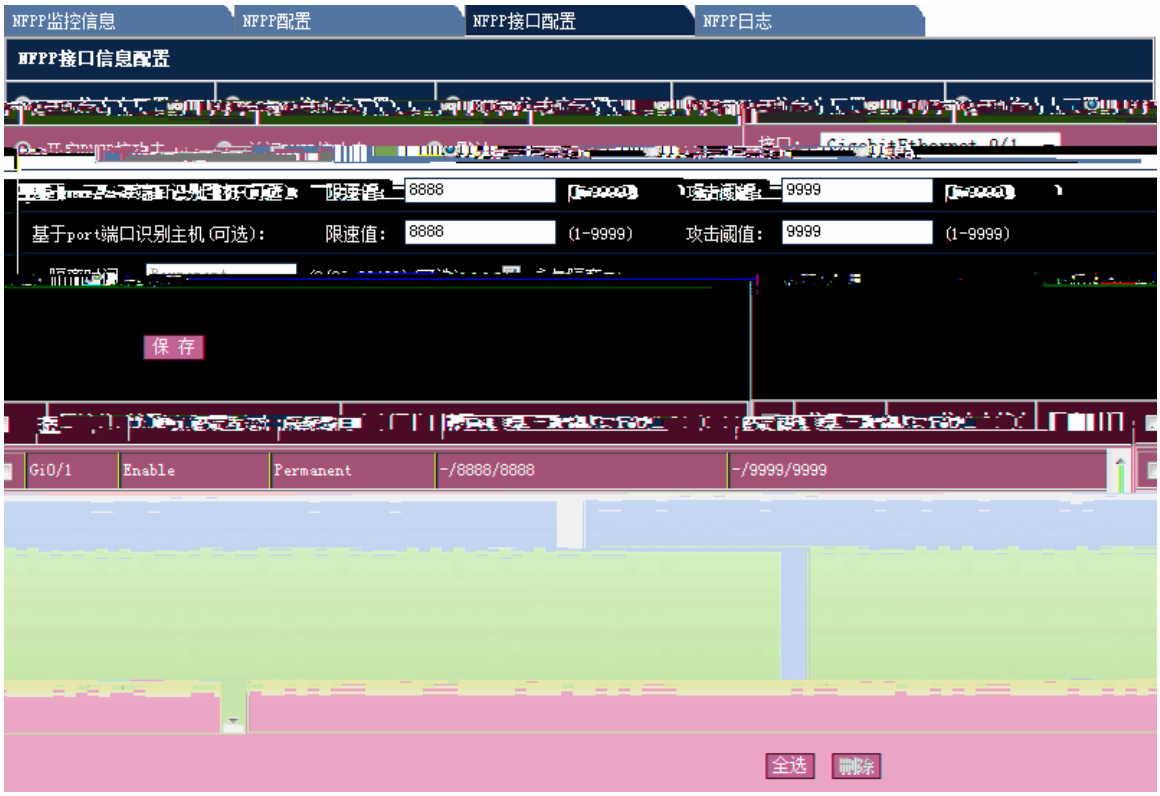
“ ”

—


NFPP接口信息配置
默认
接口: FastEthernet 0/1
开启ICMP抗攻击
1222
(1-9999)
基于ip/vid/端口识别主机(可选): 限速值: 1112 (1-9999)
2222
(1-9999)
基于port端口识别主机(可选): 限速值: 1322 (1-9999)
隔离时间: Permanent (0/30-86400)(可选)
永久隔离
保 存
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
Fa0/1
Enable
Permanent
1112/-/1322
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
基于port端口识别主机(可选):
限速值:
8888
(1-9999)
攻击阈值:
9999
(1-9999)
保 存
GiO/1
Enable
Permanent
-/8888/8888
-/9999/9999
全选
删除

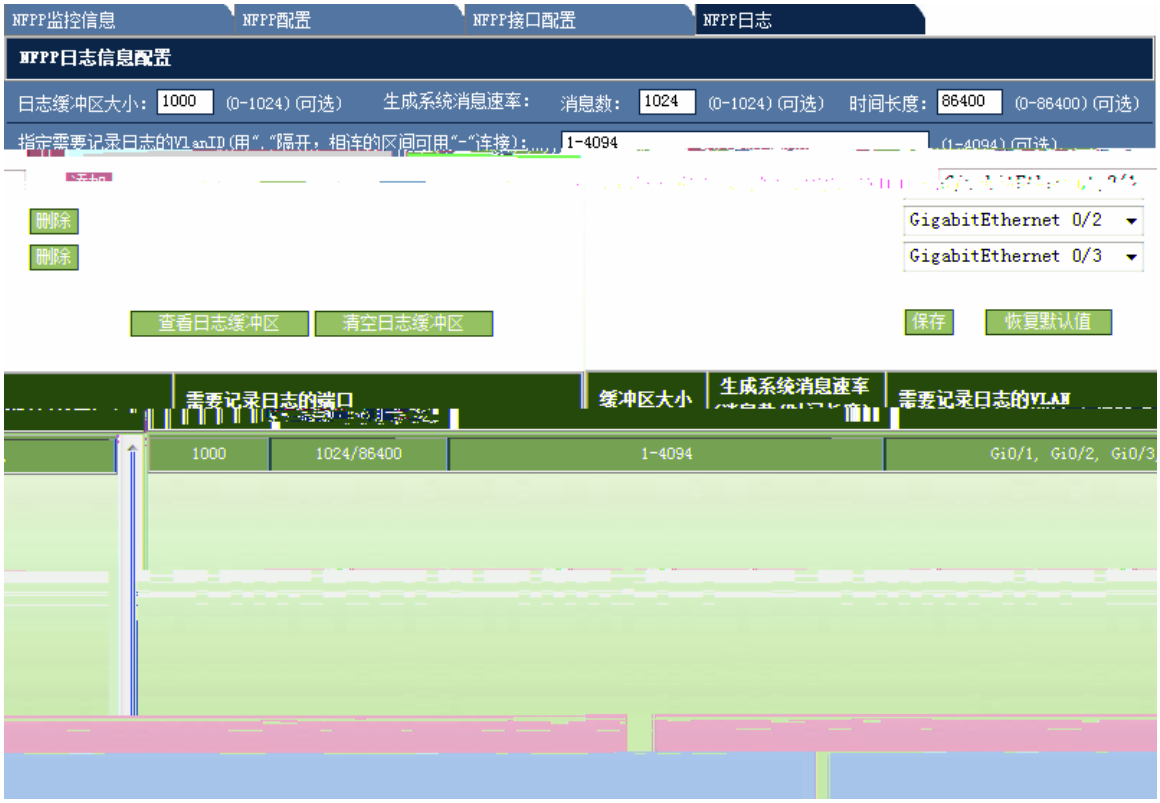
“ ”

—


NFPP监控信息
NFPP配置
NFPP接口配置
NFPP日志
NFPP接口信息配置
ARP抗攻击配置
ICMP抗攻击配置
DHCP抗攻击配置
DHCPv6抗攻击配置
ND抗攻击配置
限速值：
8888
(1-9999)
攻击阈值：
9999
(1-9999)
NS-NA模式：
保 存
Gi0/1
Enable
8888/1111/3333
9999/2222/5555
全选
删除

“ ”

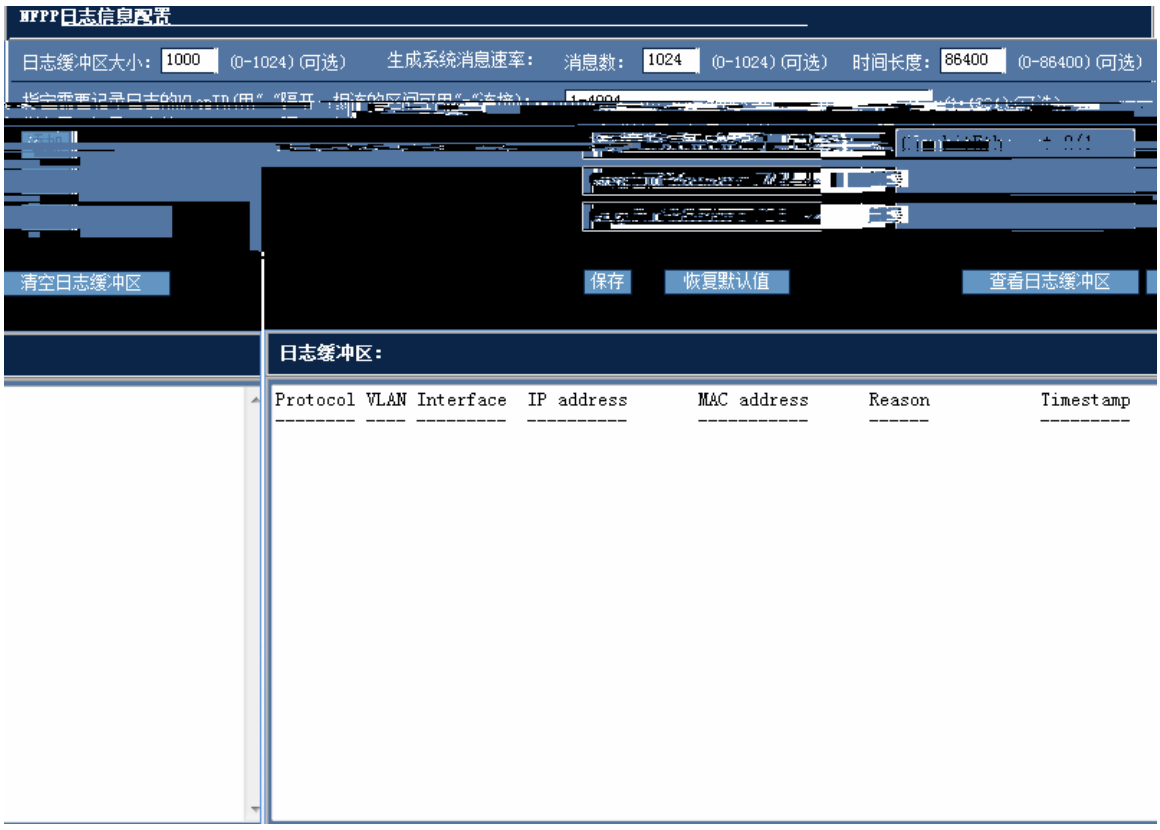
NFPP


NFPP监控信息
NFPP配置
NFPP接口配置
NFPP日志
NFPP日志信息配置
日志缓冲区大小：
1000
(0-1024)(可选)
生成系统消息速率：
消息数：
1024
(0-1024)(可选)
时间长度：
86400
(0-86400)(可选)
1-4094
删除
删除
GigabitEthernet 0/2
GigabitEthernet 0/3
查看日志缓冲区
清空日志缓冲区
保存
恢复默认值
缓冲区大小
生成系统消息速率
1000
1024/86400
1-4094

“ ”

“ ”

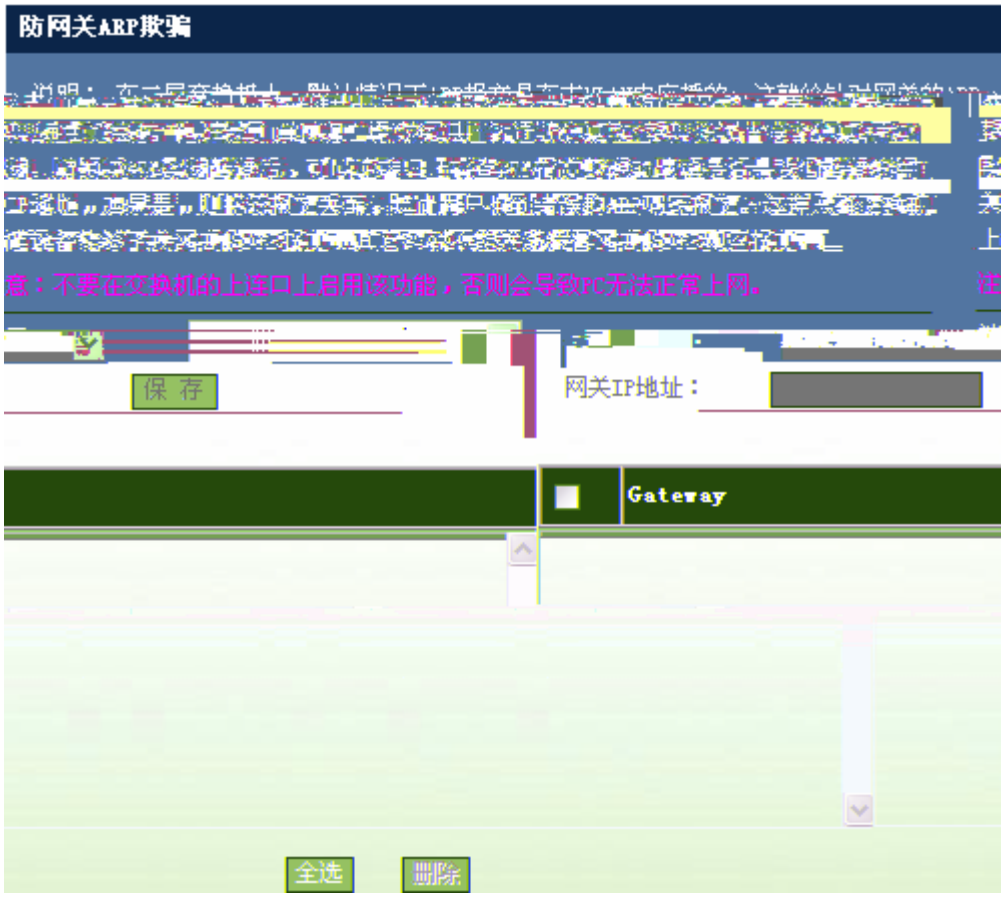
“ ”


MPPP日志信息配置
日志缓冲区大小：
1000
(0-1024) (可选)
生成系统消息速率：
消息数：
1024
(0-1024) (可选)
时间长度：
86400
(0-86400) (可选)
清空日志缓冲区
保存
恢复默认值
查看日志缓冲区
日志缓冲区：
Protocol VLAN Interface IP address MAC address Reason Timestamp

1.6

1.6.1 ARP

“ ”

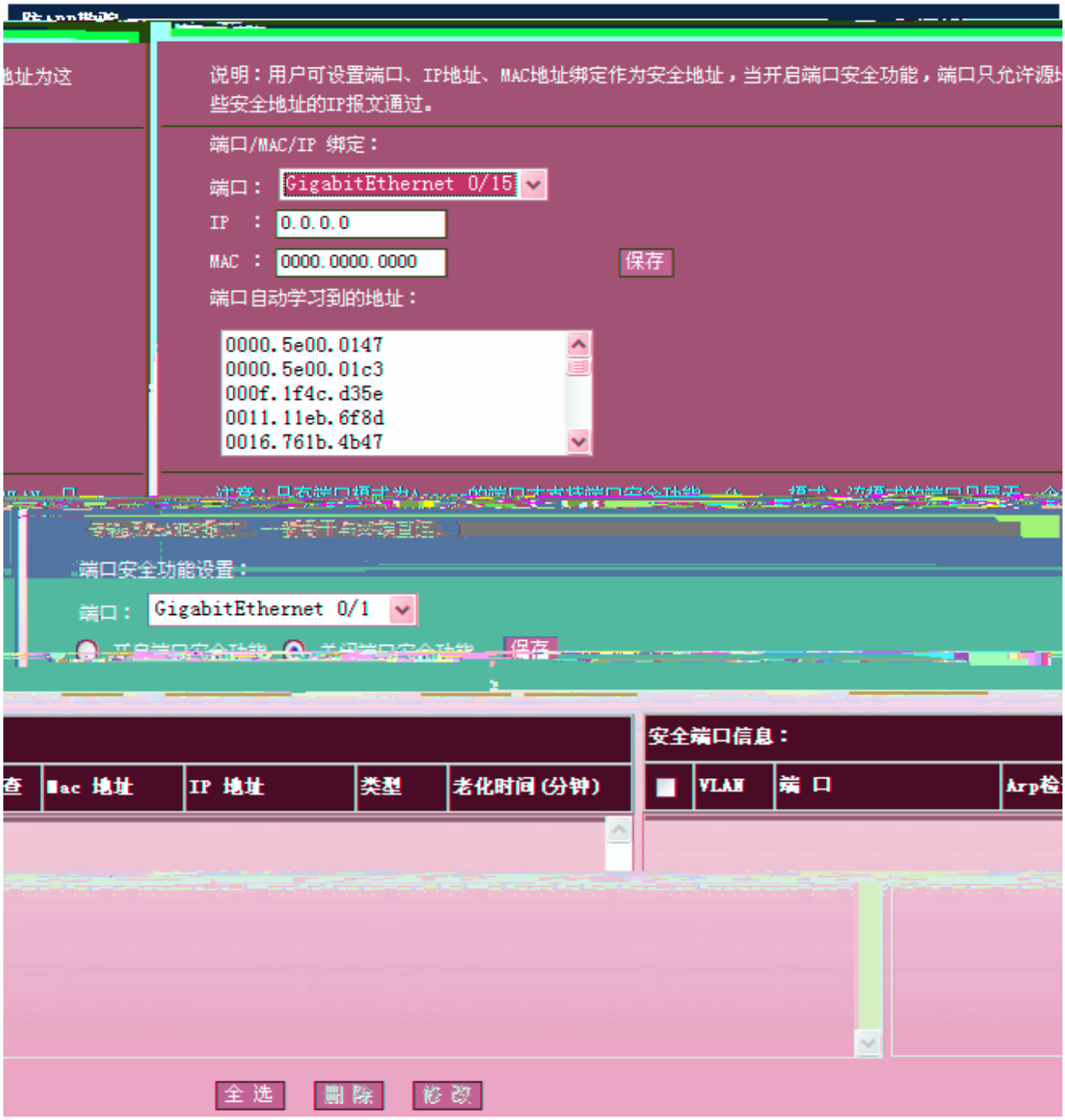

防网关ARP欺骗
意：不要在交换机的上连口上启用该功能，否则会导致PC无法正常上网。
保 存
网关IP地址：
Gateway
全选
删除

“ ”

“ ”

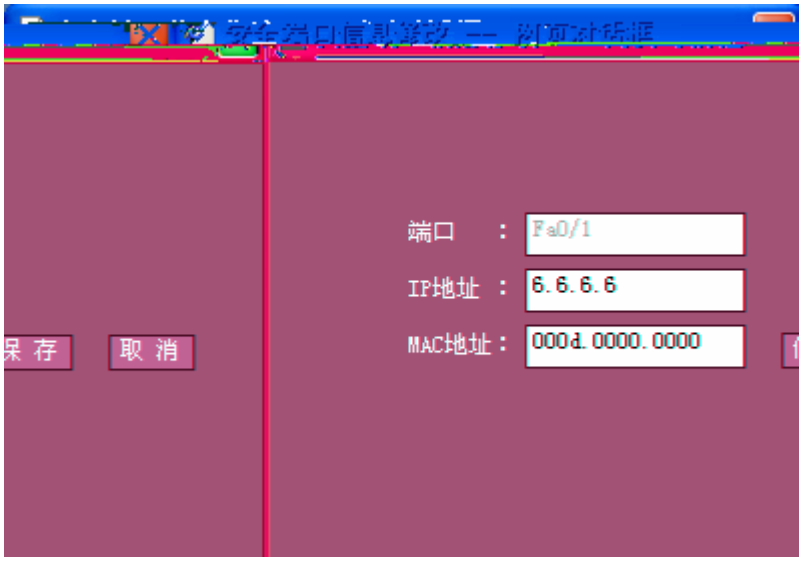
1.6.2 ARP

“ ”


地址为这
说明：用户可设置端口、IP地址、MAC地址绑定作为安全地址，当开启端口安全功能，端口只允许源
些安全地址的IP报文通过。
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
端口安全功能设置：
端口： GigabitEthernet 0/1
保存
安全端口信息：
查
Mac 地址
IP 地址
类型
老化时间(分钟)
VLAN
端 口
全 选
删 除
修 改

“ ”

“ ”



“ ”

1.6.3 APR

“ ”

“ ” “ ”

1.6.4 ACL

“ ”

ACL

“ ”

“ ” “ ”

ACL

“ ”

“ ” “ ”

“

”

“ ”

“ ” “ ”

“ ”

ACL

“ ”

“ ”

1.6.5 IP Source Guard

IP Source Guard

“ ”


接口配置
用户绑定
打开接口上的IP Source Guard功能
e 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
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
生效。
说明：IP Sourc
在DHCP Snooping
功能，功能将不
查看指定端口
查看全部
过滤类型
过滤模式
IP地址
MAC地址
VLAN
接口
ip
active
deny-all
-
-
FastEthernet 0/6
FastEthernet 0/14
全选
删除


接口配置
用户绑定
配置静态的IP源地址绑定用户
MAC地址:
VLAN:
(1-4094)
IP地址:
选择接口:
保 存
MAC地址
IP地址
租期
类型
VLAN
接口
全选
删除

1.6.6 DAI

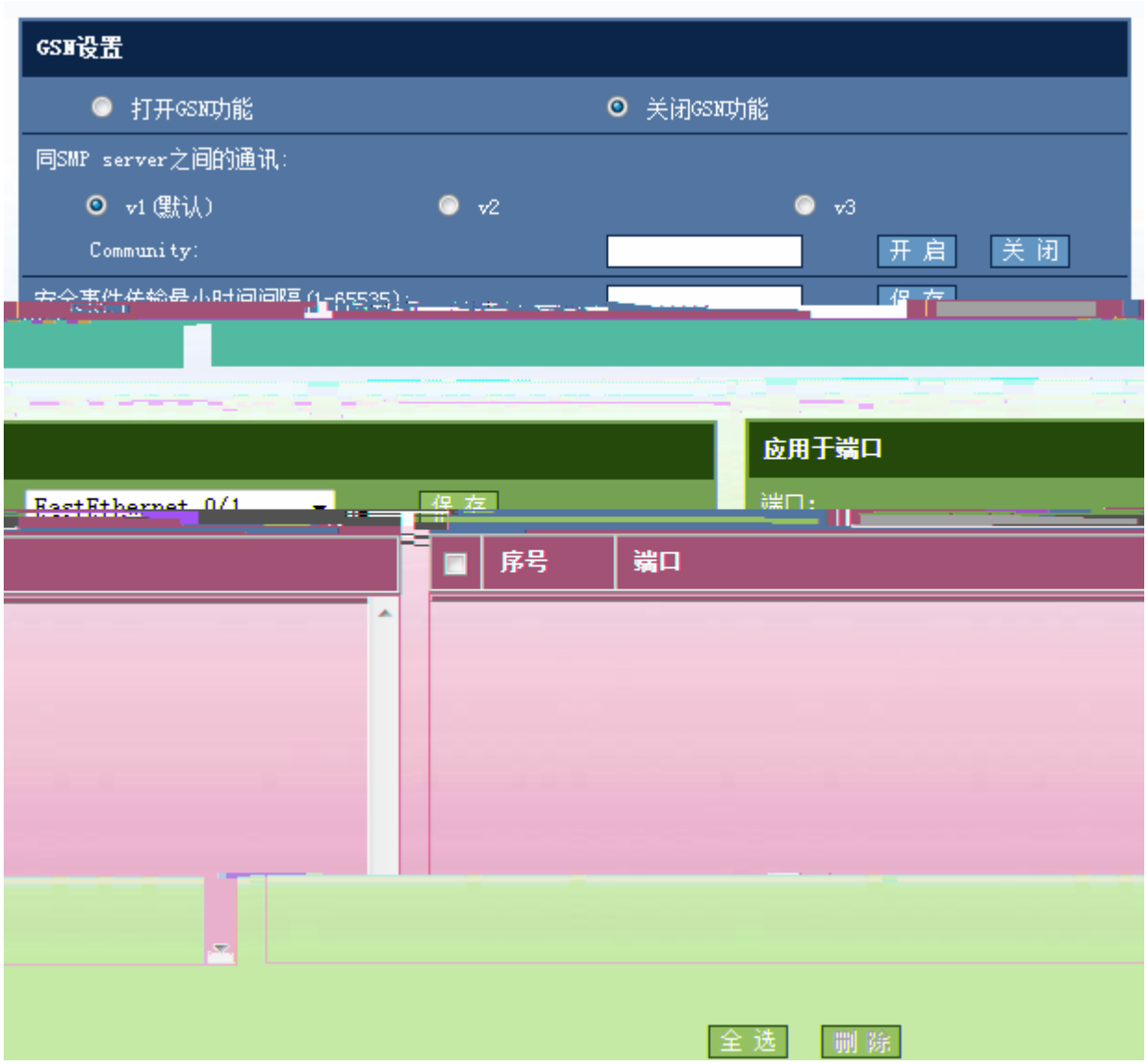
“ ”


配置指定VLAN的DAI报文检查功能
需要开启或者关闭DAI报文检查功能的VLAN ID(用','隔开，相连的区间可用'-'连接):
启用指定VLAN的DAI报文检查功能
关闭指定VLAN的DAI报文检查功能
关闭所有VLAN的DAI报文检查功能
保 存
已启用DAI报文检测功能的VLAN:
98-100,144
配置端口的信任状态
说明：此命令应用在二层接口配置模式，且此二层接口为一个SVI的成员口。
接口:
信任
不信任
保 存
各二层接口DAI配置状态
FastEthernet 0/1
Untrusted

° Ĵ ɾN Ţ V “

1.6.7 GSN

“ ”


GSN设置
打开GSN功能
关闭GSN功能
同SMP server之间的通讯:
v1(默认)
v2
v3
Community:
开 启
关 闭
应用于端口
端口:
序号
端口
全 选
删 除

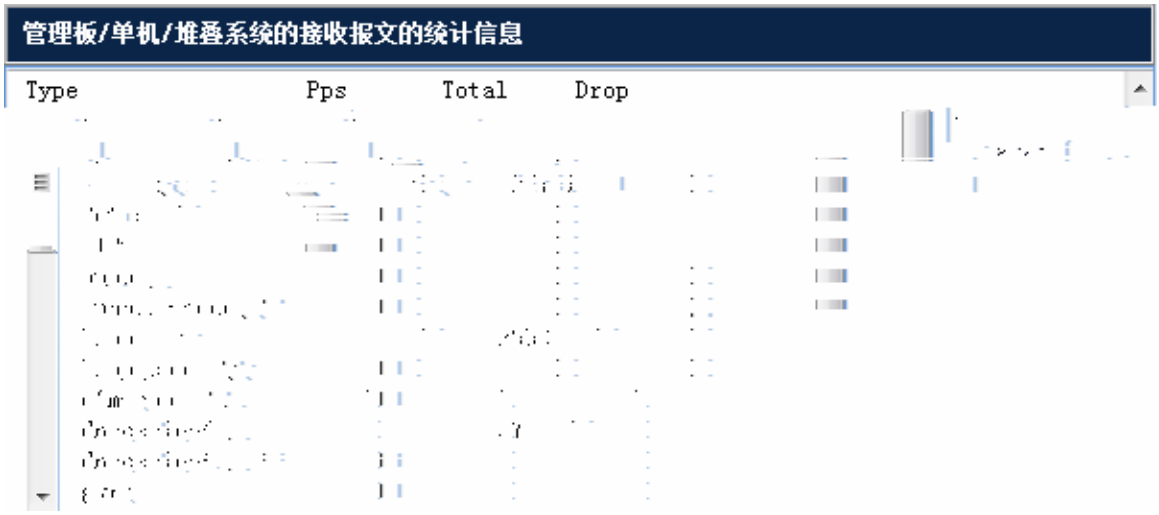
“ ”

“ ”

arp报文接收统计信息

Slot	Type	Pps	Total	Drop
MainBoard	arp	10	324430	0

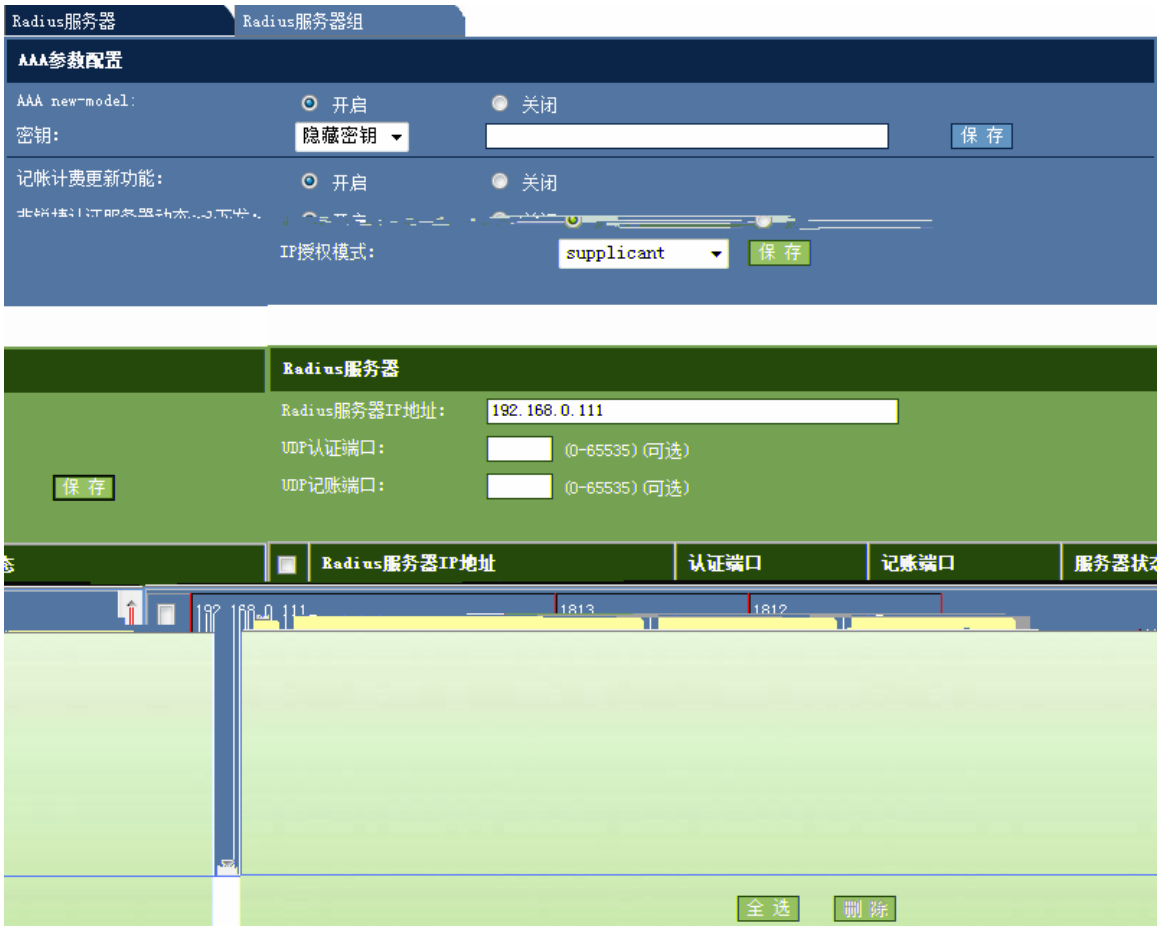
“ ”



“ ”

1.6.9 RADIUS

“ ”



RADIUS

“ ” “ ”

“ ”

“ ”

RADIUS


Radius服务器
Radius服务器组
记帐计费更新功能:
开启
关闭
非锐捷认证服务器动态acl下发:
开启
关闭
IP授权模式:
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
刷 新
Radius服务器组管理:
radius
==========Radius group radius==========
Vrf:not-set
Server:7::1
Authentication port:1812
Accounting port:1813
State:Active
Server:::1
Authentication port:1812
Accounting port:1813
State:Active
Server:::
Authentication port:1812
Accounting port:1813
State:Active


AAA配置
应用AAA方法
基于域名的AAA服务
高级配置
AAA设置
提示：系统当前已开启“aaa new-model”，若不需要用到AAA配置，可以选择关闭!
关 闭
Radius服务器
本地数据库(用户管理)
authentication
none
保 存
全 选

AAA

“ ” “ ”

“ ”

AAA

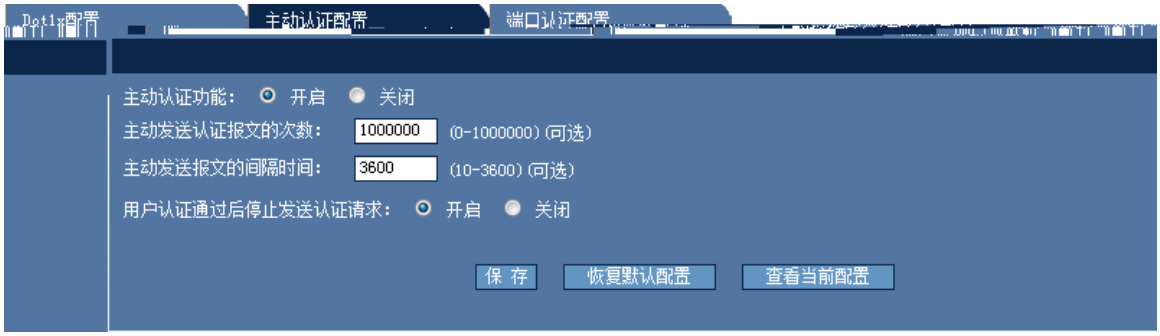

AAA配置
应用AAA方法
基于域名的AAA服务
高级配置
基于域名的AAA服务
default
default
default
default
2
删除
==========Domain default==========
State: Block
Username format: With-domain
Access limit: 2
802.1X Access statistic: 0
Selected method list:
authentication dot1x default
authentication ppp default
authorization network default

“ ”

“ ”

“ ”

“ ” “ ”


Dot1x配置
主动认证配置
端口认证配置
主动认证功能： 开启 关闭
主动发送认证报文的次数： 1000000 (0-1000000) (可选)
主动发送报文的间隔时间： 3600 (10-3600) (可选)
用户认证通过后停止发送认证请求： 开启 关闭
保 存
恢复默认配置
查看当前配置

ñ ” ǎ ㄐ ú ɜ̌


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。
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：
FastEthernet 0/1
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

“ ” “ ”

“ ”

“ ”

“ ”

“ ”

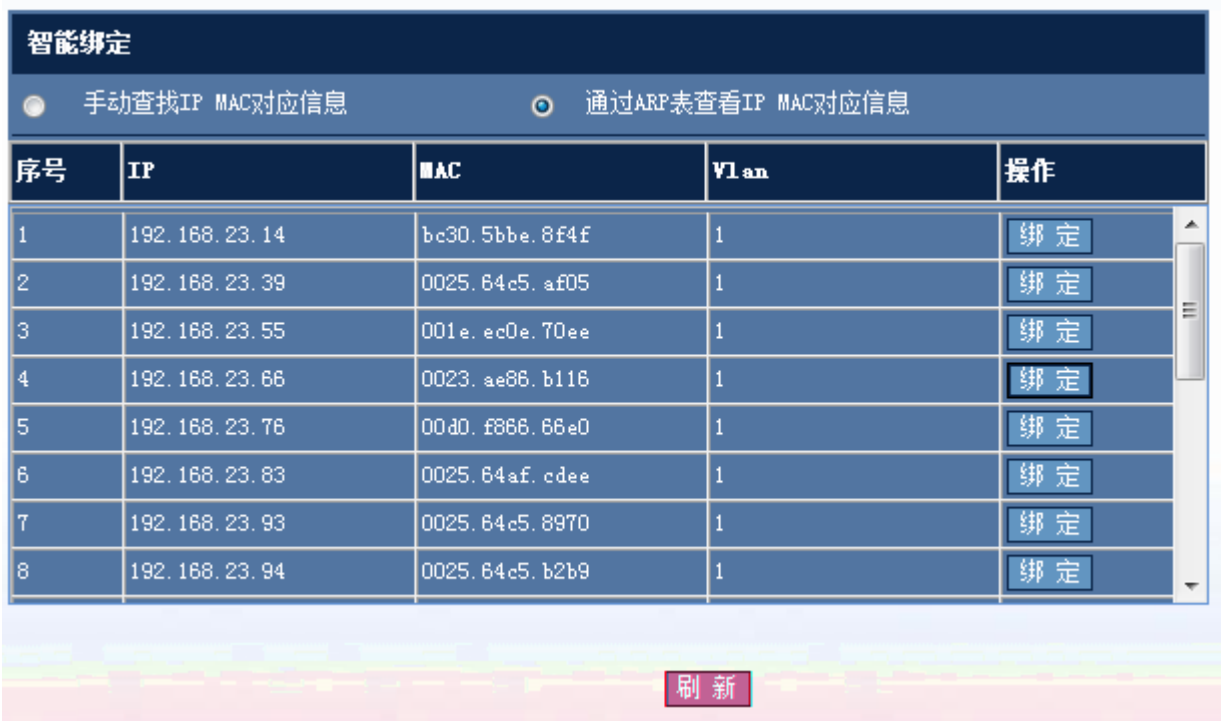
1.6.12

“ ”


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
MAC地址:
绑 定
序号
IP
MAC
全 选
删 除
刷 新

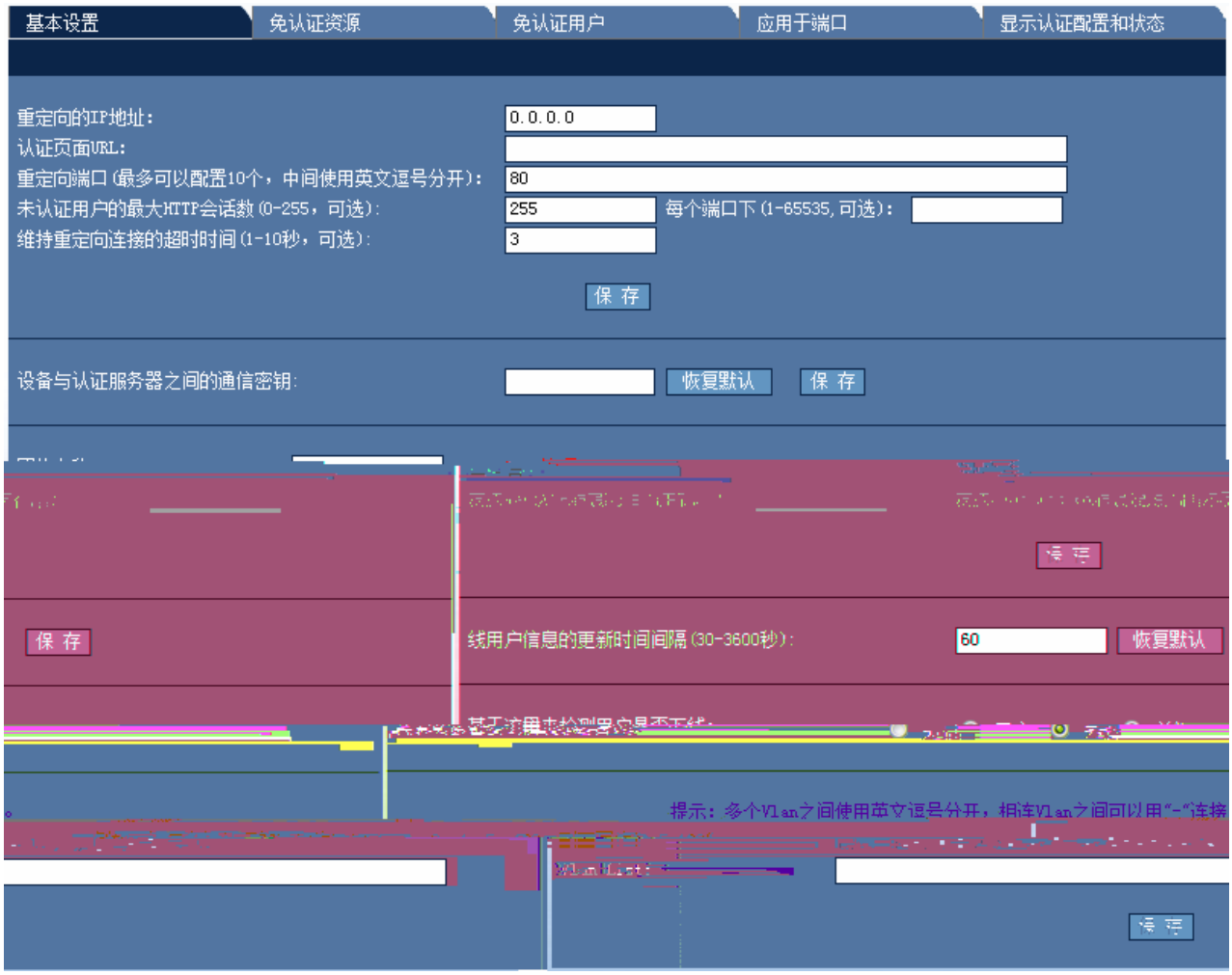
“ ”

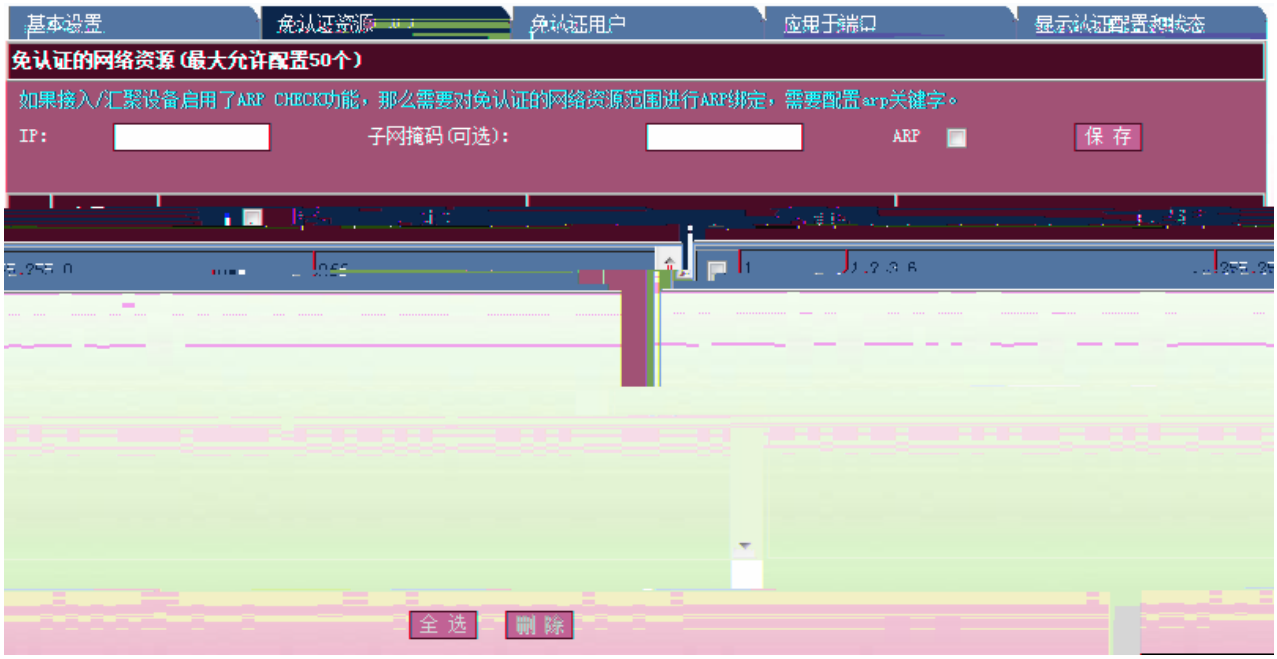
“ ”


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

1.6.13 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（1-65535，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


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
免认证的网络资源(最大允许配置50个)
如果接入/汇聚设备启用了ARP CHECK功能，那么需要对免认证的网络资源范围进行ARP绑定，需要配置arp关键字。
IP:
子网掩码(可选):
ARP
保 存
全 选
删 除

“ ”

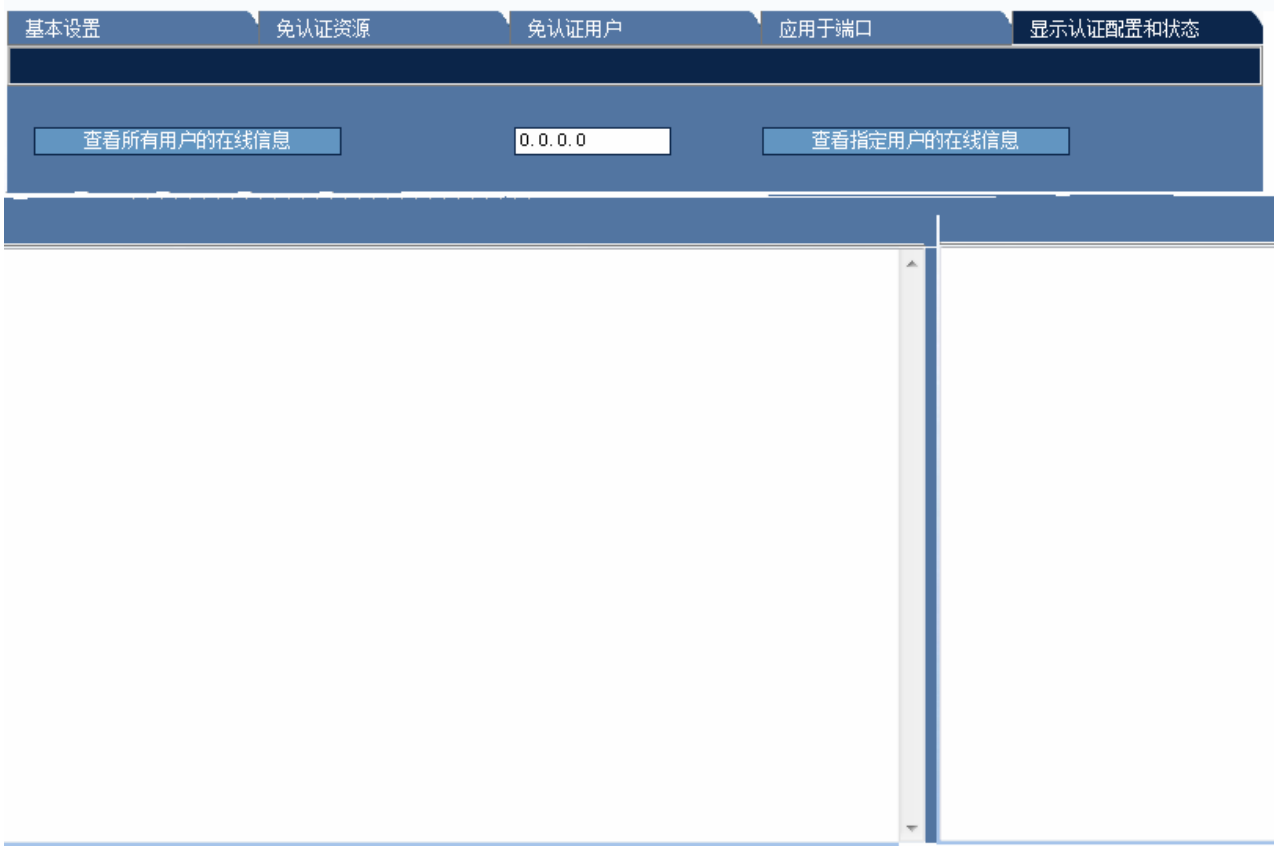

免认证用户(最大允许配置50个)
子网掩码
端口
ARP绑定
序号
IP地址
255.255.255.0
Fa0/2
On
1
192.168.23.1

“ ”

“ ”


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

“ ” “ ”


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
查看所有用户的在线信息
0.0.0.0
查看指定用户的在线信息

1.6.14 DHCP Snooping

“ ”

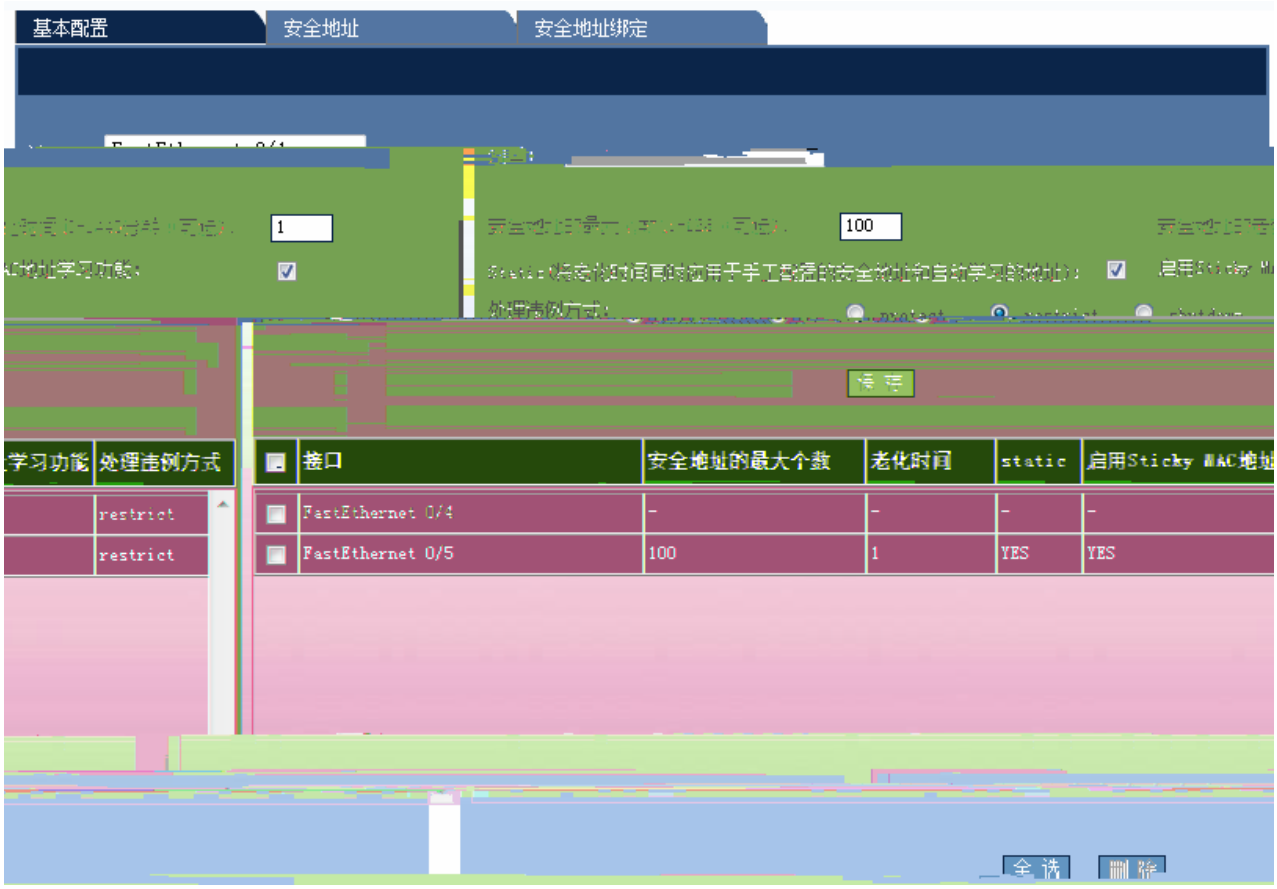
1.7.2

1.7.3

“ ”

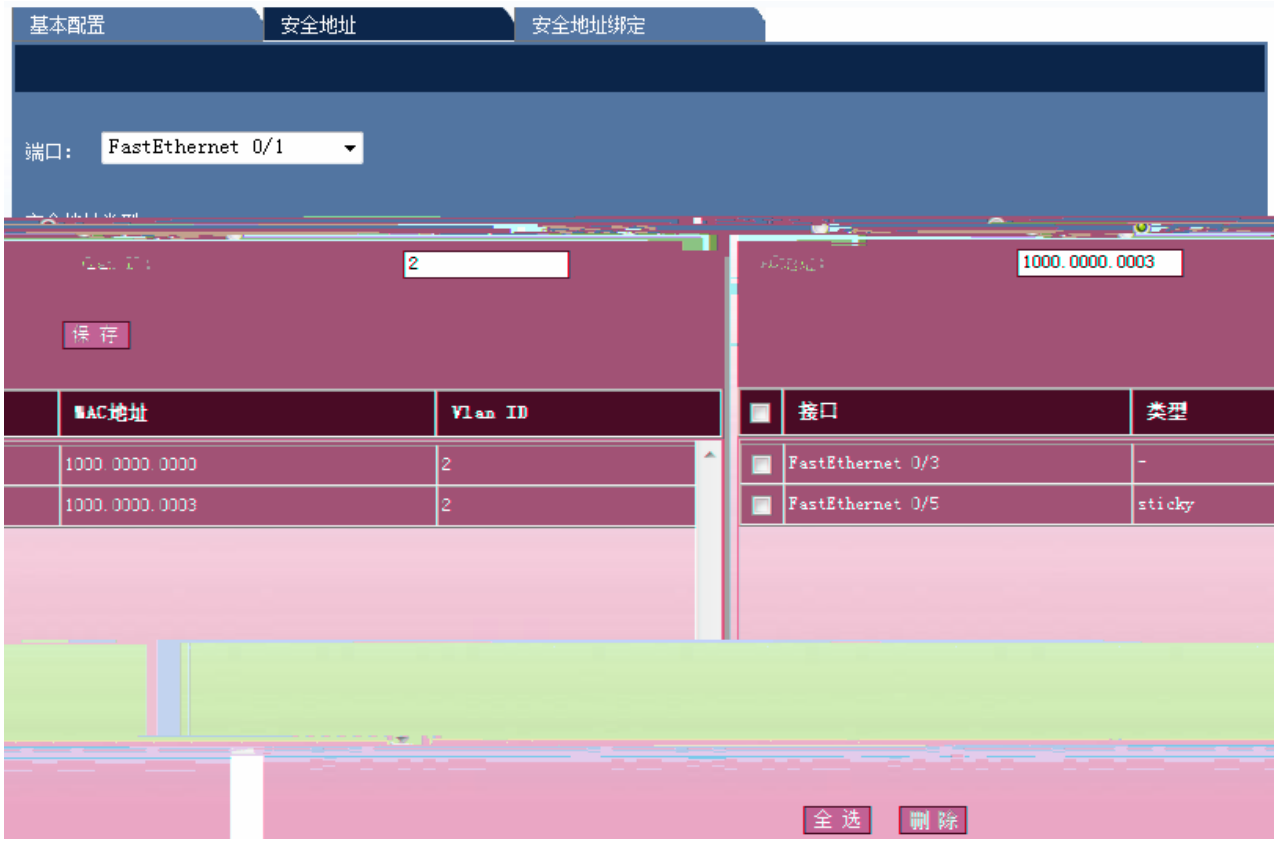

流设置
说明：应用策略设置对端口的输入或输出流进行限制。
端 口：
FastEthernet 0/1
策略列表：
（策略设置）
限速方向：
输入限速
输出限速
保存
端口
方向
策略名
信任模式
COS
FastEthernet 0/1
FastEthernet 0/2
FastEthernet 0/3
FastEthernet 0/4
FastEthernet 0/5
FastEthernet 0/6
FastEthernet 0/7
FastEthernet 0/8
FastEthernet 0/9
FastEthernet 0/10
FastEthernet 0/11
全选
删除

“ ” “ ”


基本配置
安全地址
安全地址绑定
1
100
处理违例方式
restrict
restrict
接口
安全地址的最大个数
老化时间
static
FastEthernet 0/4
FastEthernet 0/5
100
1
YES
YES
全选

“ ”

“ ”


基本配置
安全地址
安全地址绑定
端口：
FastEthernet 0/1
2
1000.0000.0003
保 存
MAC地址
Vlan ID
接口
类型
1000.0000.0000
2
FastEthernet 0/3
-
1000.0000.0003
2
FastEthernet 0/5
sticky
全 选
删 除

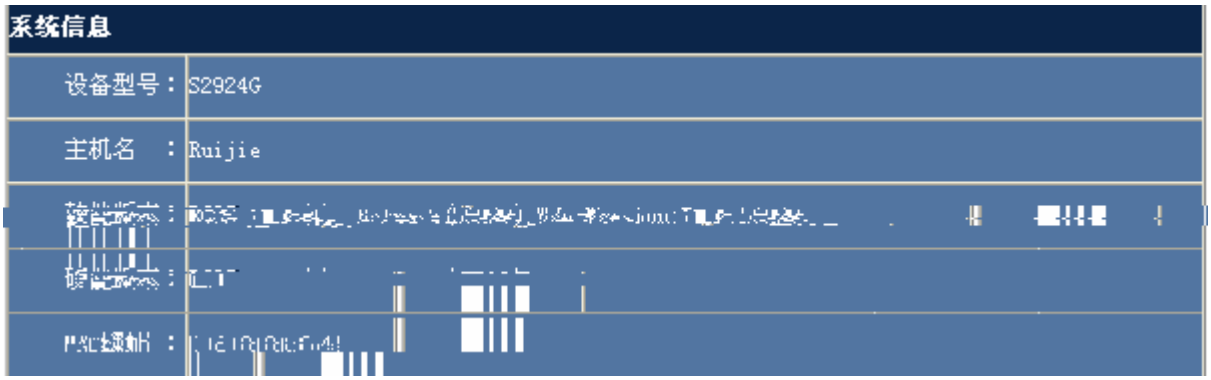
“ ”

“ ”


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
1000.0000.0000
10
1.2.3.3
FastEthernet 0/1
删 除
全 选

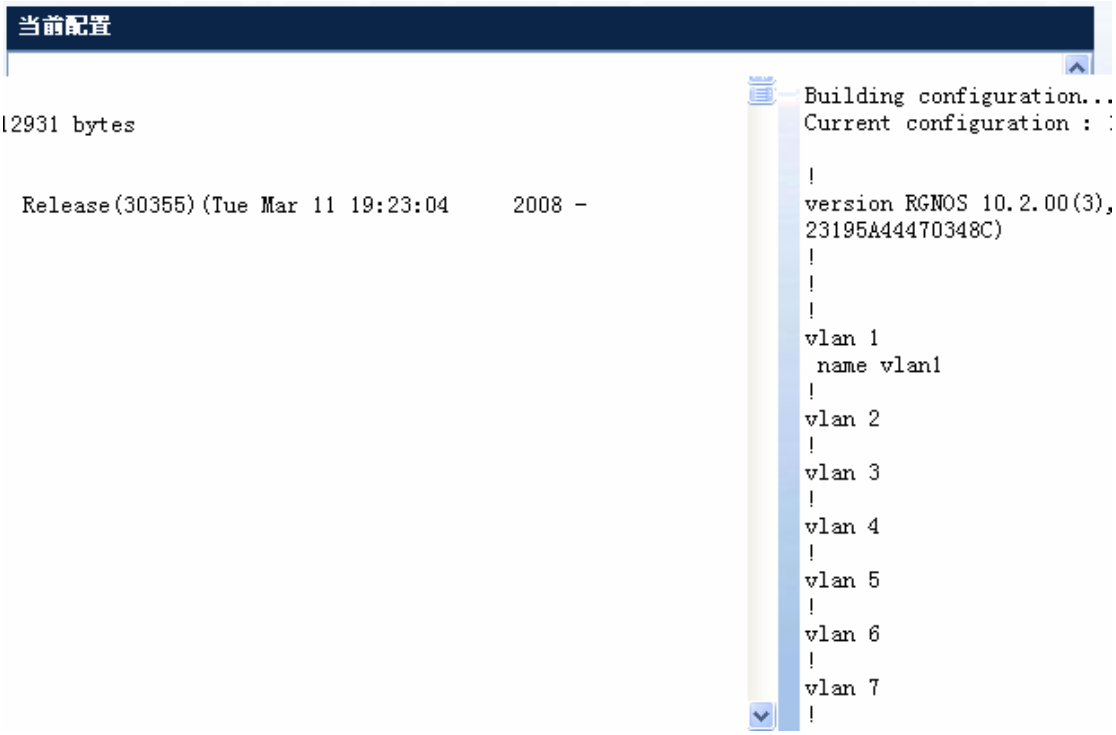
“ ”

“ ”


系统信息
设备型号：S2924G
主机名 ：Ruijie

1.8.2

“ ”


当前配置
12931 bytes
Release(30355)(Tue Mar 11 19:23:04 2008 -
Building configuration...
Current configuration :
!
version RGNOS 10.2.00(3),
23195A44470348C)
!
!
!
vlan 1
name vlan1
!
vlan 2
!
vlan 3
!
vlan 4
!
vlan 5
!
vlan 6
!
vlan 7
!

1.8.3

“ ”

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

1.8.4

“ ”

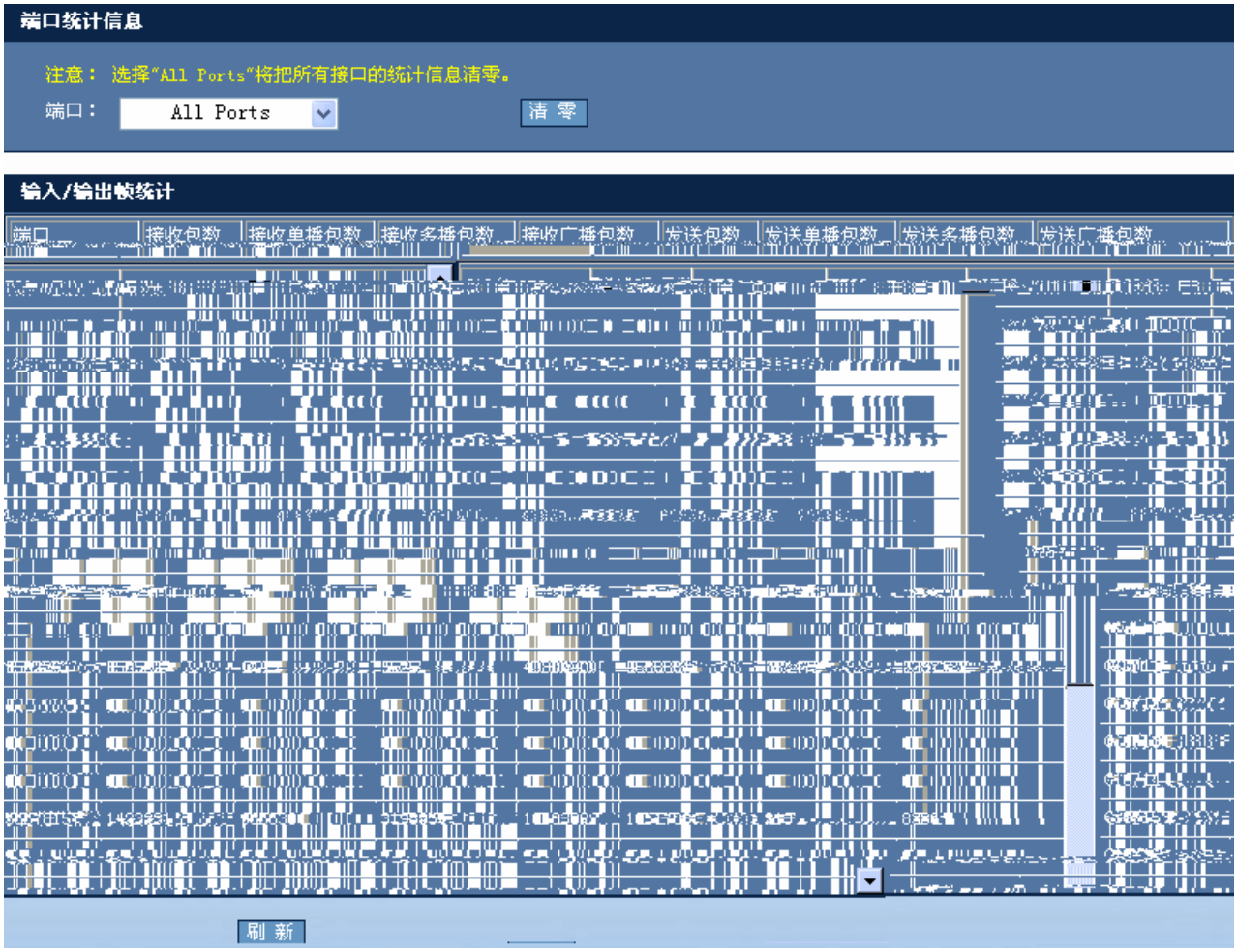
端口运行状态

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

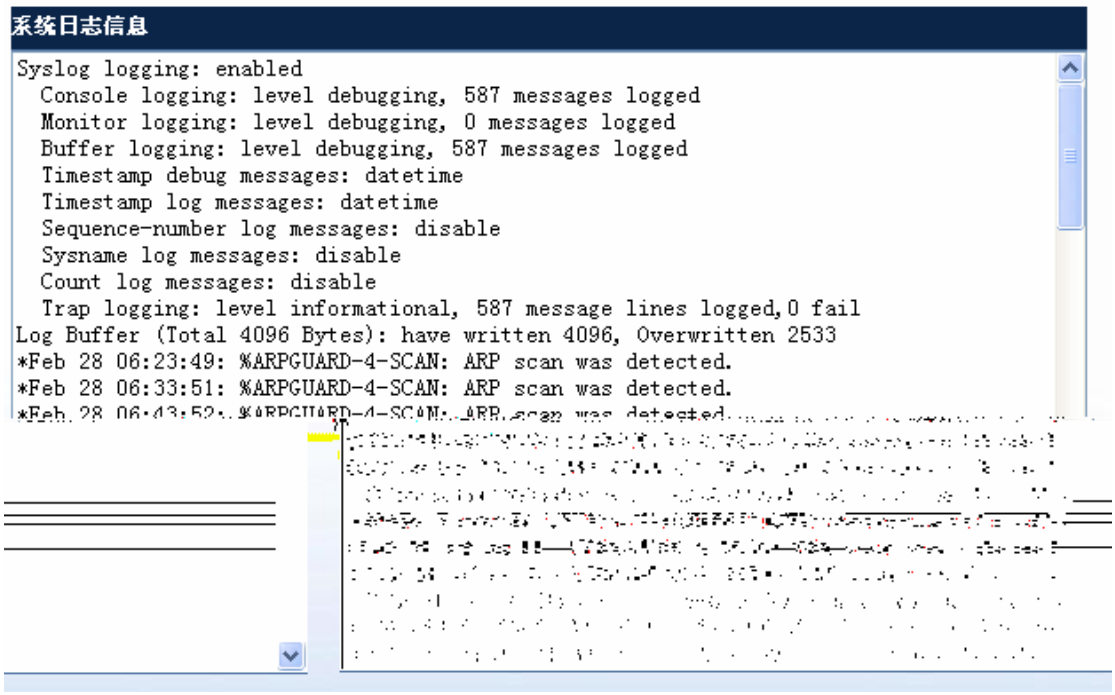
1.8.5

“ ”


端口统计信息
注意： 选择"All Ports"将把所有接口的统计信息清零。
端口：
All Ports
清 零
输入/输出帧统计
端口
接收包数
接收单播包数
接收多播包数
接收广播包数
发送包数
发送单播包数
发送多播包数
发送广播包数
刷 新

1.8.6

“ ”


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.

1.9

1.9.1 Ping

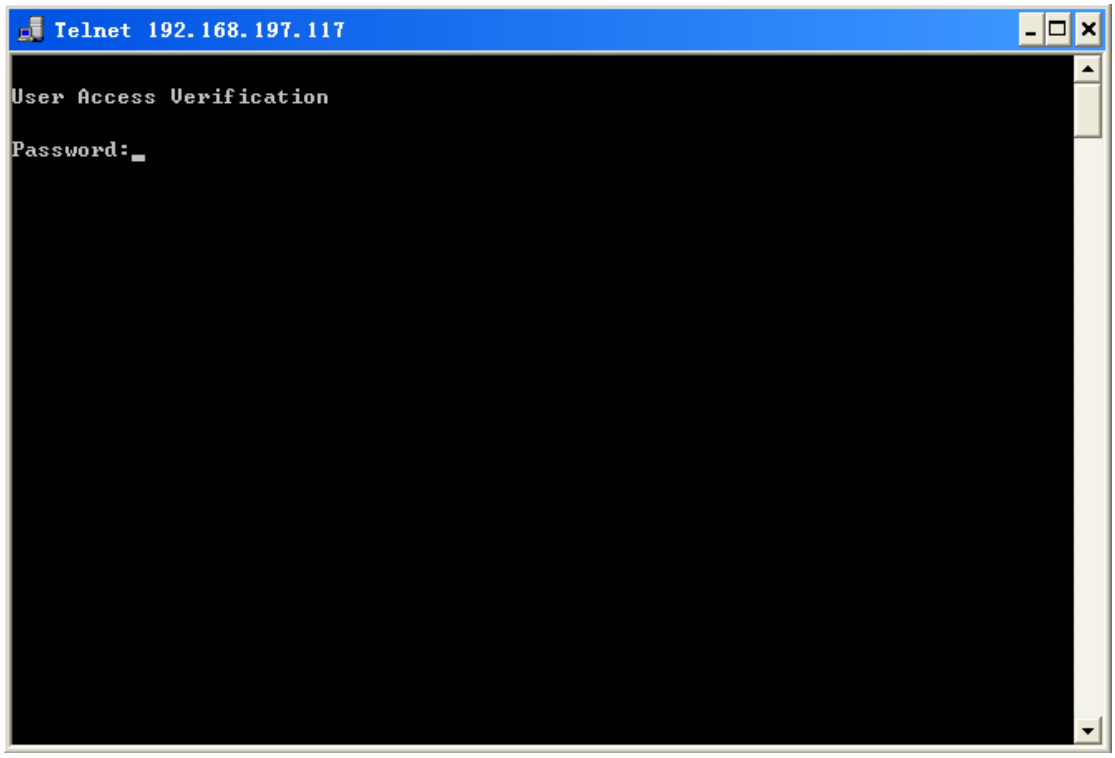
“ ”


Ping
IP：
0.0.0.0
开 始
结果：

“ ”

1.9.2 Telnet

“ ”



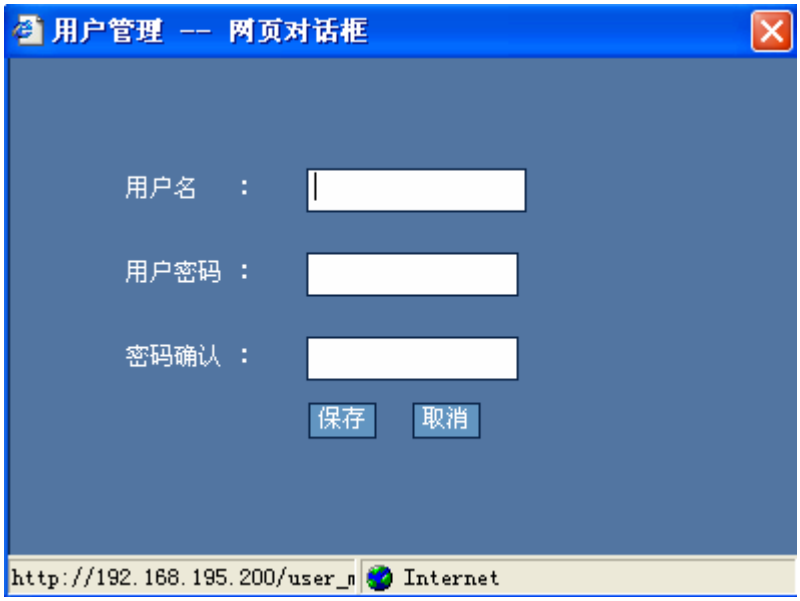
“ ”

1.9.3

“ ”


用户管理
序号
用户名
1
admin
添加用户
全 选
删 除
修 改

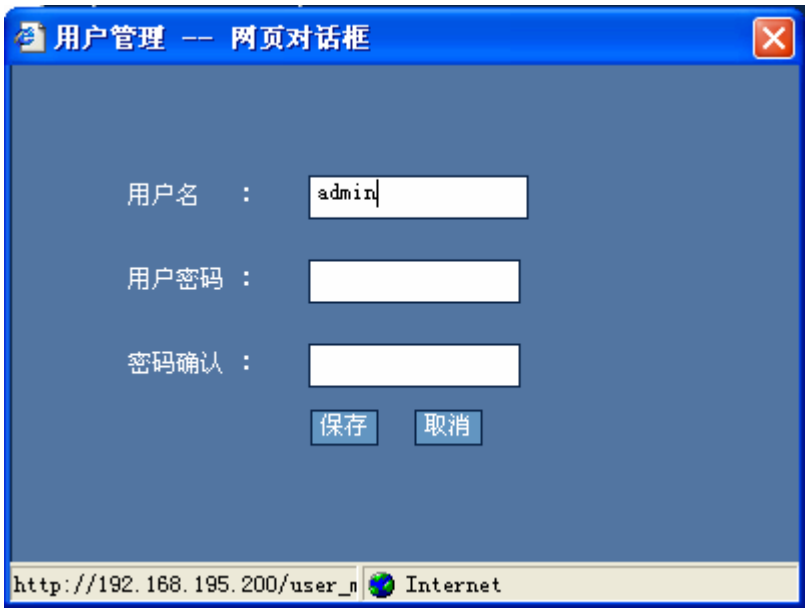
“ ”


用户管理 -- 网页对话框
用户名 ：
用户密码 ：
密码确认 ：
保存
取消
http://192.168.195.200/user_m
Internet

“ ”

“ ”

“ ”


用户管理 -- 网页对话框
用户名 ：
admin
用户密码 ：
密码确认 ：
保存
取消
http://192.168.195.200/user_n
Internet

“ ”

1.9.4

“ ”


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

“ ”

“ ”

1.9.5 /

“ ”

“ ”

ξ Ɗ FTP ξ Ɗ FTP N ʊ

```
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)#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
```

```
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
```