



WEB a Â Õ Å

RG-AS2GT x æ @ & ²

RGOS 10.4(2b12)p4

g é • - Y u V1.0

• Ñ f

©2015



± • Ñ f

ø W

• $\bar{y} f$

RGOS 10.4 (2b12)p4

~ À * Š

ê ± V

<http://www.ruijie.com.cn/>

<http://webchat.ruijie.com.cn>

<http://www.ruijie.com.cn/service.aspx>

7× 24

4008-111-000

<http://support.ruijie.com.cn>

service@ruijie.com.cn

ü » ž j

- / ,

1)

[] []

{x|y|...}

[x|y|...]

//

2)

1 WEB

WEB

IE

WEB

WEB

WEB

WEB

WEB

WEB

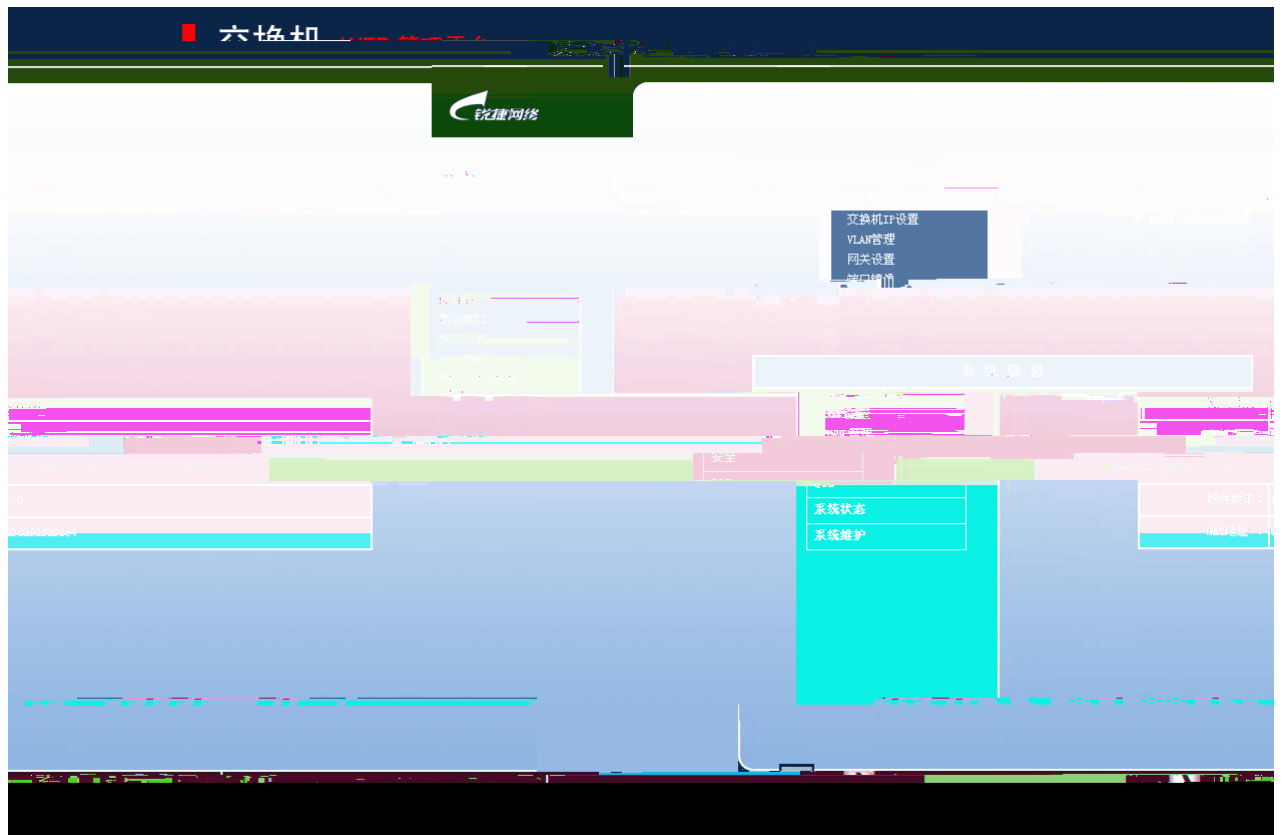
IE

2



2

WEB



3 WEB



WEB





5 IP

IP

2.2.2 VLAN

VLAN

1 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上独立的广播域，每个逻辑广播域就是一个VLAN。

<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

6 VLAN

VLAN

VLAN

VLAN

VLAN管理 -- 网页对话框

VLAN ID : (1-4094)

VLAN 名称 : (可选)

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

9 VLAN

VLAN ID

2.2.3

11

2.2.5



12

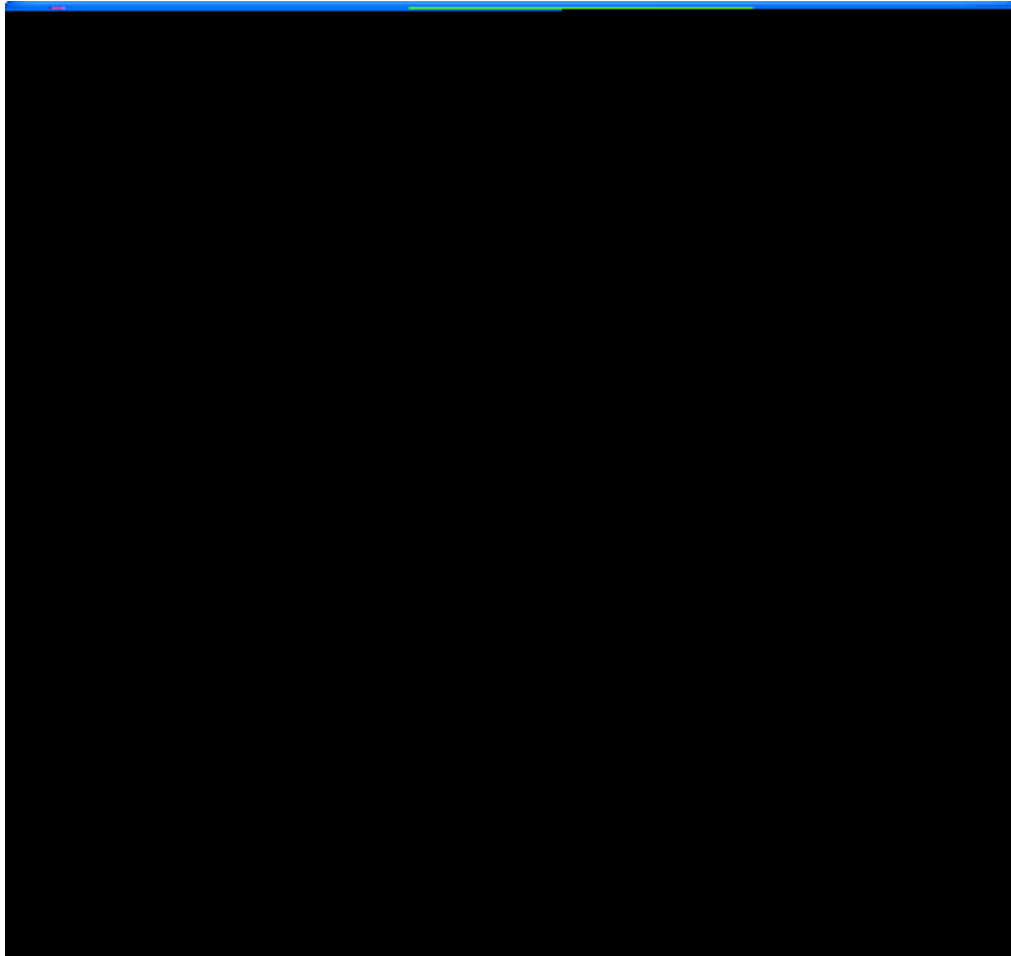
2.2.6



13

1

2



14

3

2.2.7

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 (M)	流控	描述
Gi0/1	Down	Half	10	On	-
FastEthernet0/24	Down	Auto	100	Auto	
FastEthernet0/23	Down	Auto	100	Auto	
FastEthernet0/22	Down	Auto	100	Auto	
FastEthernet0/21	Down	Auto	100	Auto	
FastEthernet0/20	Down	Auto	100	Auto	
FastEthernet0/19	Down	Auto	100	Auto	
FastEthernet0/18	Down	Auto	100	Auto	
FastEthernet0/17	Down	Auto	100	Auto	
FastEthernet0/16	Down	Auto	100	Auto	
FastEthernet0/15	Down	Auto	100	Auto	
FastEthernet0/14	Down	Auto	100	Auto	
FastEthernet0/13	Down	Auto	100	Auto	
FastEthernet0/12	Down	Auto	100	Auto	
FastEthernet0/11	Down	Auto	100	Auto	
FastEthernet0/10	Down	Auto	100	Auto	
FastEthernet0/9	Down	Auto	100	Auto	
FastEthernet0/8	Down	Auto	100	Auto	
FastEthernet0/7	Down	Auto	100	Auto	
FastEthernet0/6	Down	Auto	100	Auto	
FastEthernet0/5	Down	Auto	100	Auto	
FastEthernet0/4	Down	Auto	100	Auto	
FastEthernet0/3	Down	Auto	100	Auto	
FastEthernet0/2	Down	Auto	100	Auto	
FastEthernet0/1	Down	Auto	100	Auto	

15

2.2.8 DHCP

DHCP

DHCP



16 DHCP

1) / DHCP

/ DHCP

2) DHCP

DHCP

DHCP

2.2.9 IGMP Snooping

IGMP Snooping

IGMP Snooping



SNMP



19 SNMP

SNMP

SNMP

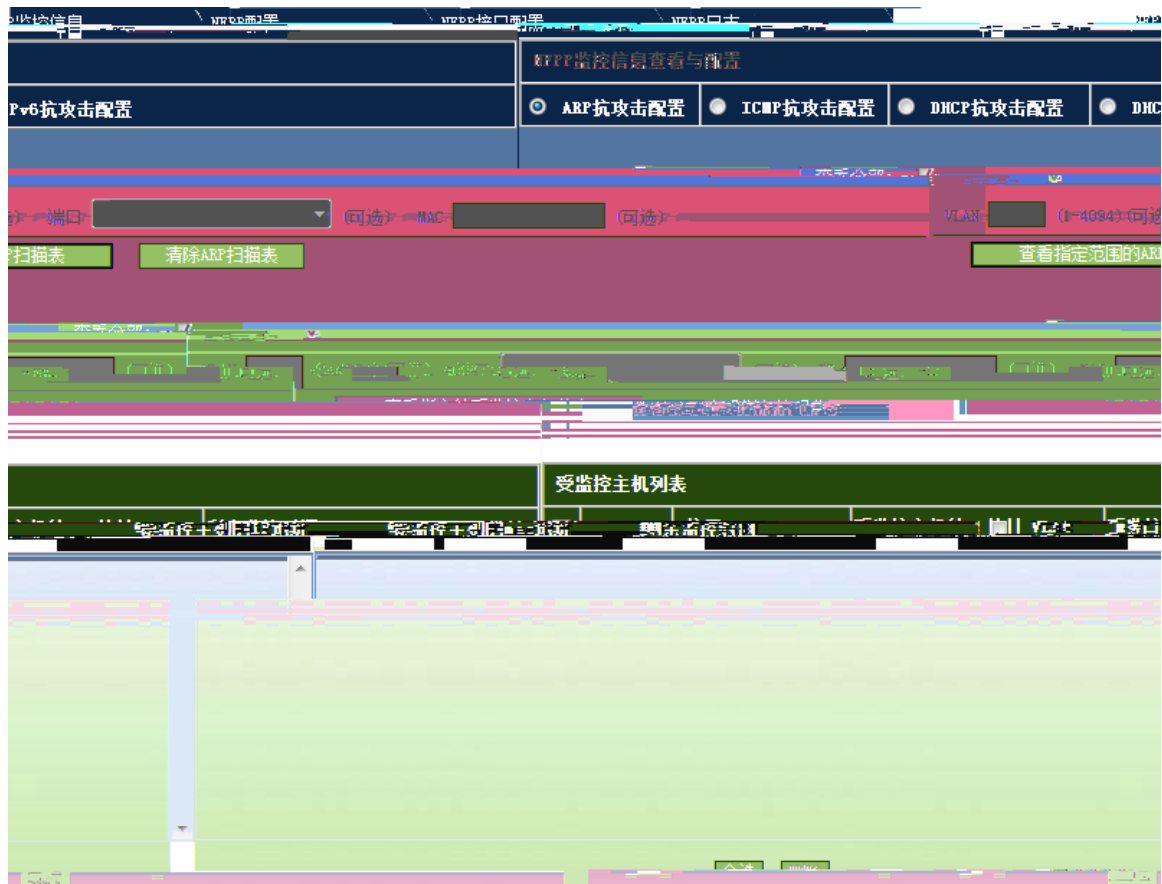
SNMP

SNMP

2.2.12 NFPP

NFPP

1 NFPP



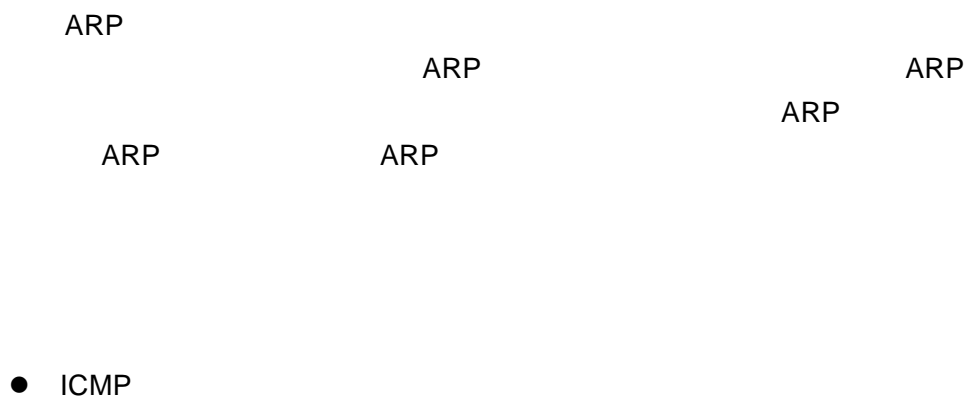
20 NFPP

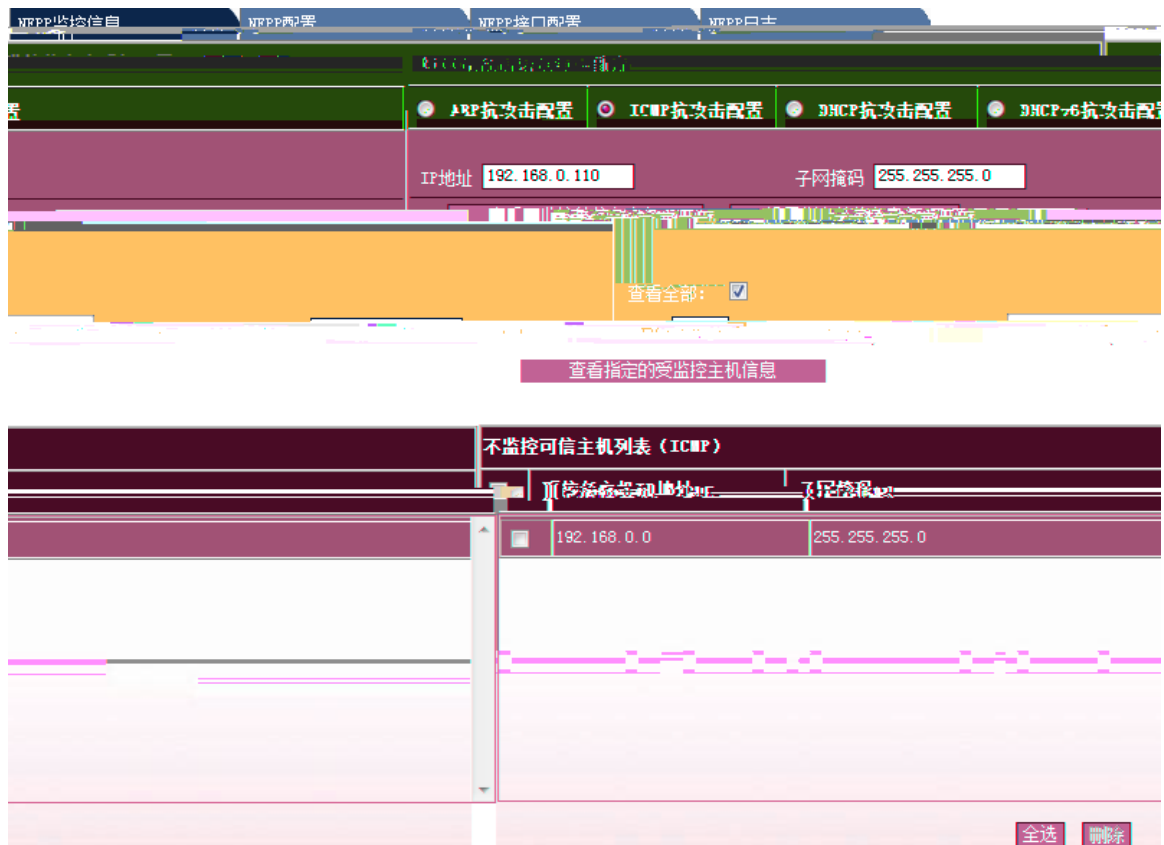
- ARP

ARP扫描表信息

IP address	MAC address	timestamp	VLAN	interface
-	001a.a942.f27f	2016-6-6 11:8:53	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	1	Fa0/40
-	001a.a942.f27f	2016-6-6 11:17:13	1	Fa0/40
-	001a.a942.f27f	2016-6-6 11:18:14	1	Fa0/40
-	001a.a942.f27f	2016-6-6 11:19:15	1	Fa0/40
-	001a.a942.f27f	2016-6-6 11:20:23	1	Fa0/40
-	001a.a942.f27f	2016-6-6 11:21:24	1	Fa0/40
-	001a.a942.f27f	2016-6-6 11:22:24	1	Fa0/40
-	001a.a942.f27f	2016-6-6 11:23:25	1	Fa0/40
-	001a.a942.f27f	2016-6-6 11:25:34	1	Fa0/40

21 ARP





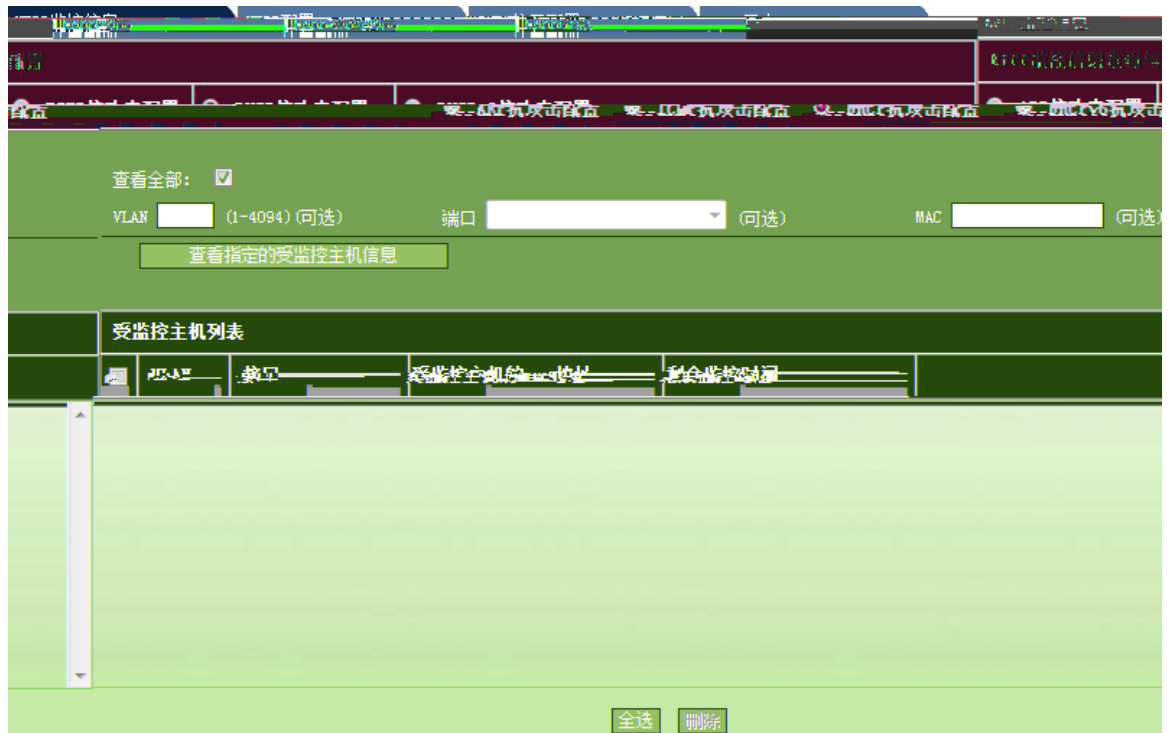
22 NFPP

--ICMP

ICMP

IP

- DHCP



23 NFPP — DHCP

DHCP

- DHCPv6

NFPP监控信息 NFPP配置 NFPP接口配置 NFPP日志

Protocol	Report Ratio	Report Max Bandwidth	Route Report Max Bandwidth	Report Max Bandwidth	Protocol Report Ratio	Route Report Ratio
	-	-	-	-	-	-

修改 恢复默认

协议类型: ARP ICMP DHCP

Protocol	DHCPv6	ND	ARP	ICMP	DHCP
Enable	Enable	Enable	Enable	Enable	Enable
0	0	0	-	-	0
600s	600s	600s	-	-	600s
1000	1000	1000	-	-	1000
100	100	100	15/15/15	-	4/4/1
100	100	100	30/30/30	-	8/8/2
-	-	-	-	-	15

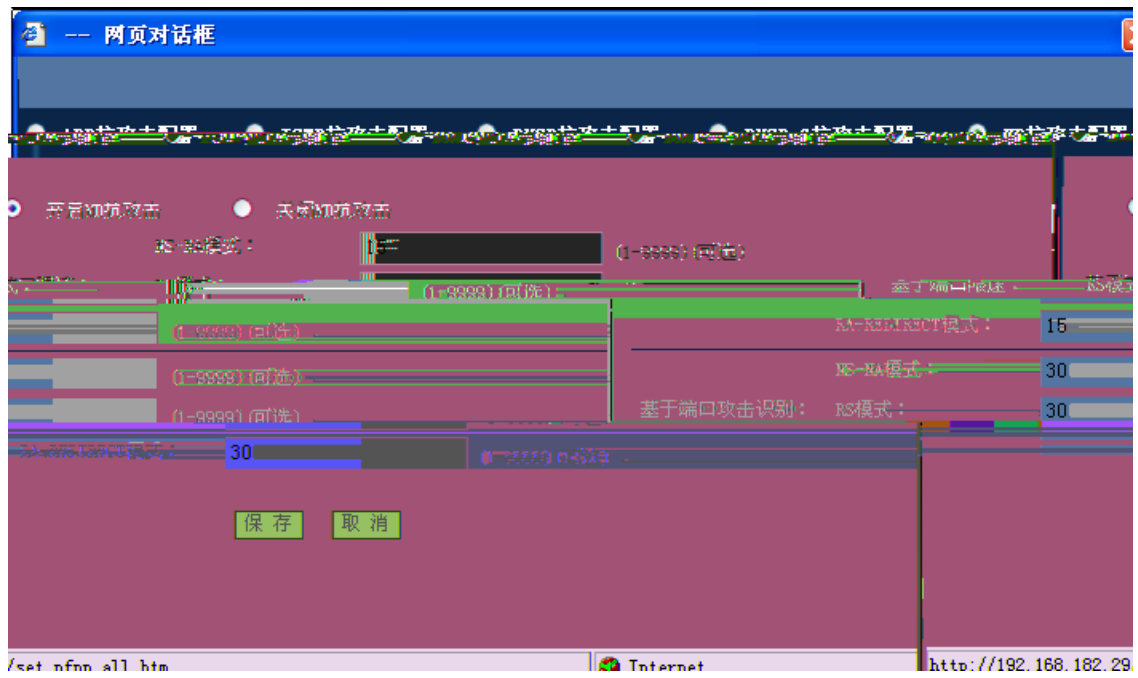
状态: 恢复默认 恢复默认 恢复默认 恢复默认 恢复默认

攻击阈值 (基于ip识别/基于mac识别/全局端口): 恢复默认

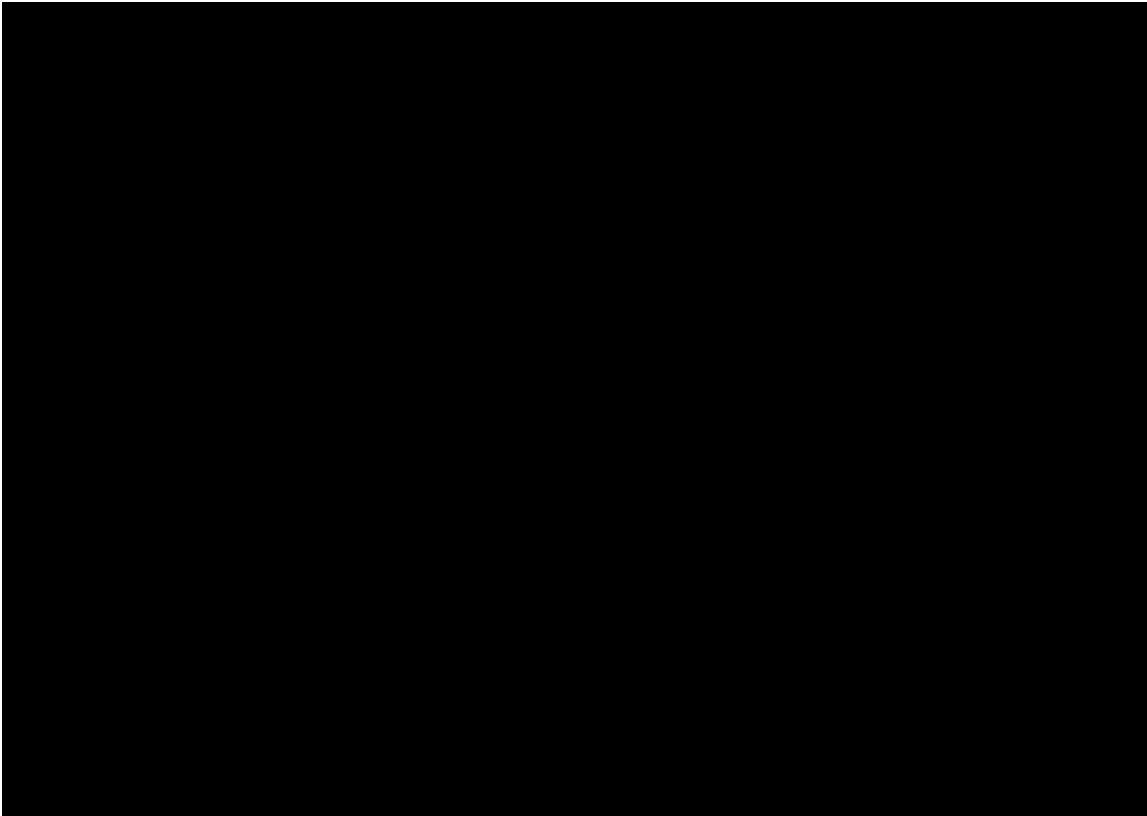
扫描阈值: 恢复默认

修改 恢复默认

25 NFPP NFPP 4



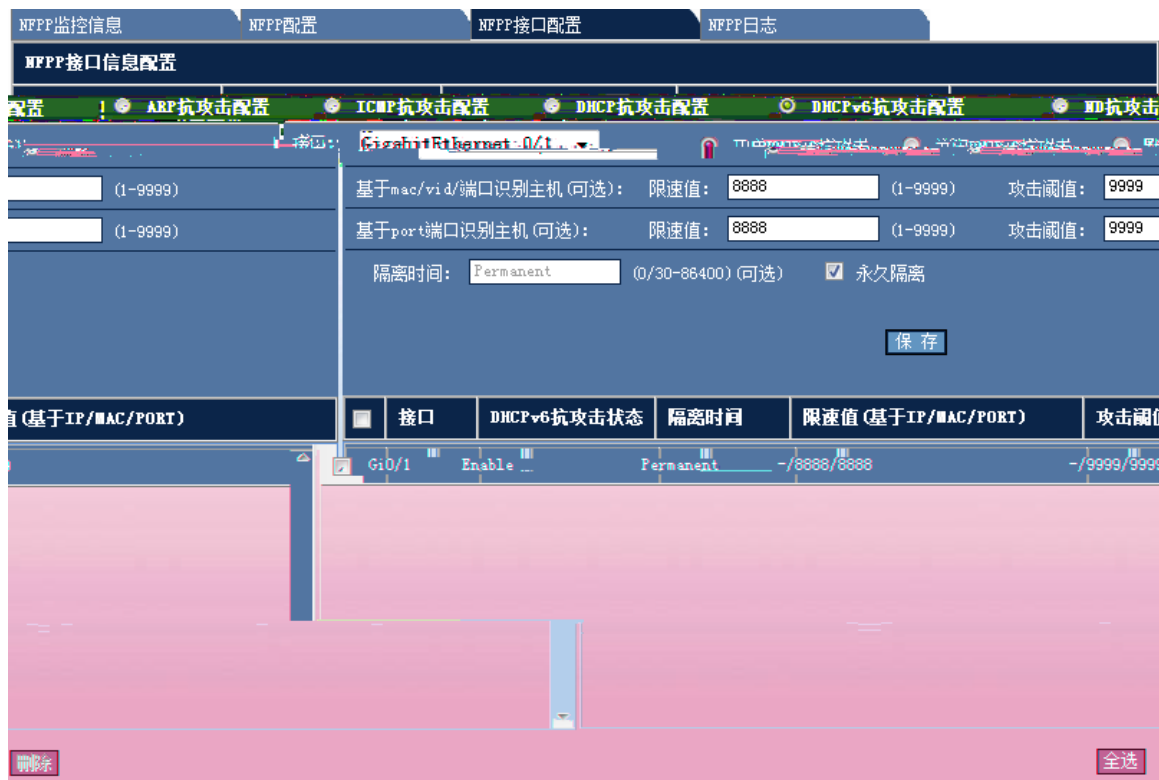
27 NFPP



28 NFPP —NFPP ARP

ARP NFPP

- ICMP



31 NFPF — NFPF DHCPv6

DHCPv6 NFPF

- ND

配置

指定需要记录日志的VLAN ID (用“-”隔开，相连的区间可用“-”连接): (1-4094) (可选)

指定需要记录日志的端口 (可选)

GigabitEthernet 0/1

GigabitEthernet 0/2

GigabitEthernet 0/3

速率 (长度)	需要记录日志的VLAN	需要记录日志的端口	缓冲区大小	生成系统消息 消息数/时间
10	1-4094	Gi0/1, Gi0/2, Gi0/3,	1000	1024/8640

33 NFPP

NFPP



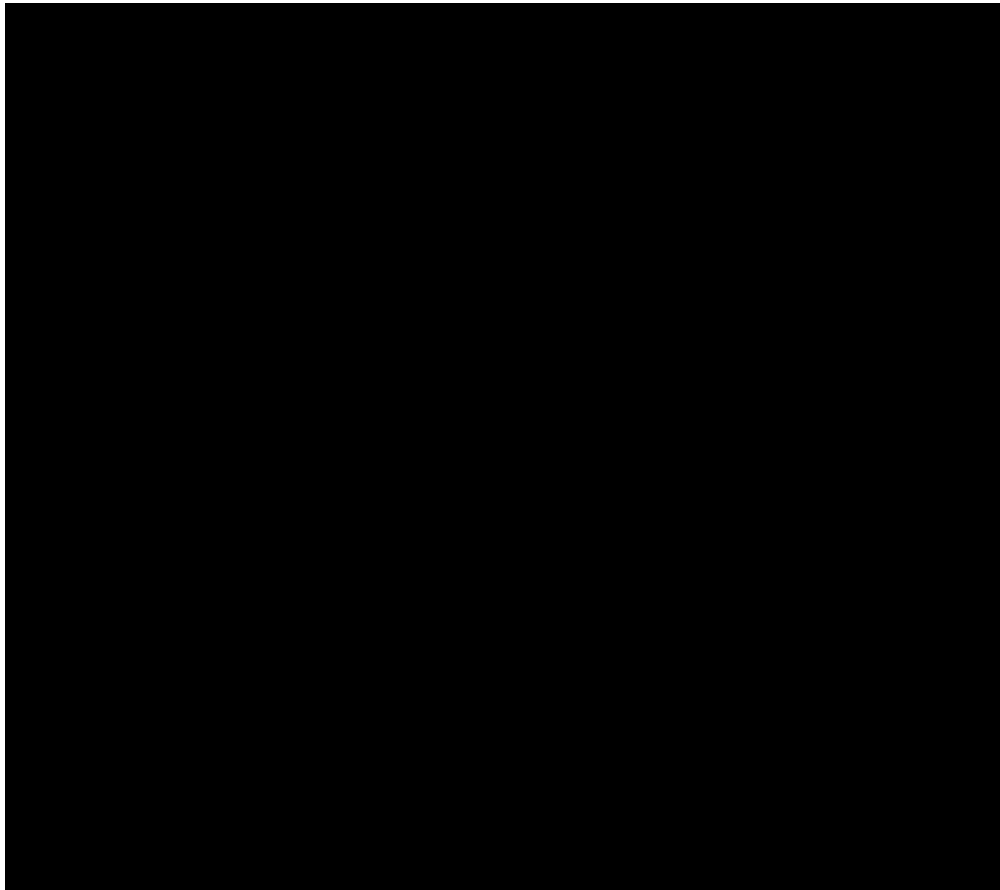
34

2.3

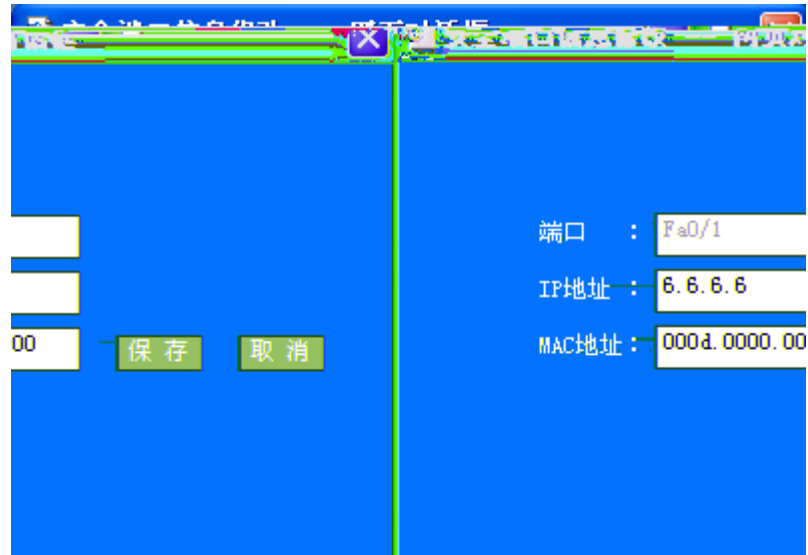
2.3.1 ARP

ARP

ARP



3)



37

2.3.3 APR

ARP

ARP



38 ARP

ARP

ARP

2.3.4 ACL

ACL

ACL



39 ACL

1 ACL

ACL
ACL

ACL ACE
ACL ACE

ACL ACE
ACL

2 ACL ACE

IP

IP

IP

显示ACL信息 **ACL配置** 将ACL应用于端口

ACL配置

配置ACL规则的基本格式为：[ACL ID] rule [rule-id] [permit/deny] [protocol] [source IP address] [source mask] [destination IP address] [destination mask] [time-range] [action]

配置掩码规定了当一个IP地址与其他的IP地址进行比较时，该IP地址中哪些位应该被忽略。通配符掩码中的“1”表示忽略IP地址中“1”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：

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： 通配符掩码： (可选)

40 IP

ID

IP IP , IP

 IP IP

IP



41 IP

ID

TCP UDP IP ICMP

IP

IP

IP

IP

IP

IP

3 ACL



42 ACL

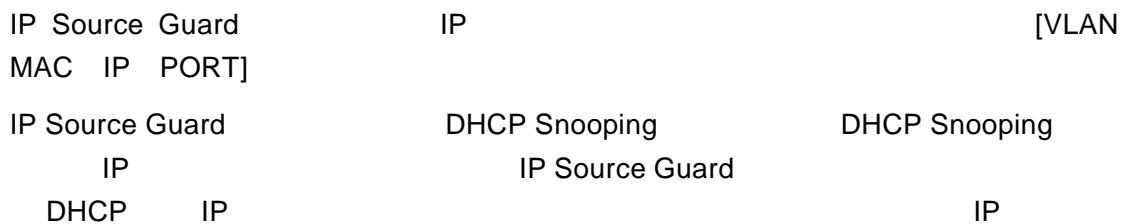
ACL

ACL



2.3.5 IP Source Guard

IP Source Guard:



IP Source Guard DHCP Snooping
 DHCP Snooping

IP Source Guard

IP Source Guard



43 IP Source Guard

1

IP Source Guard

IP+MAC

IP+MAC

()

2

IP

MAC MAC
 VLAN VLAN ID
 IP IP

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

1.2.3.4	infinite	static	1	FastEthernet 0/4	<input type="checkbox"/>	00d0.f811.2233
---------	----------	--------	---	------------------	--------------------------	----------------

全选 删除

44

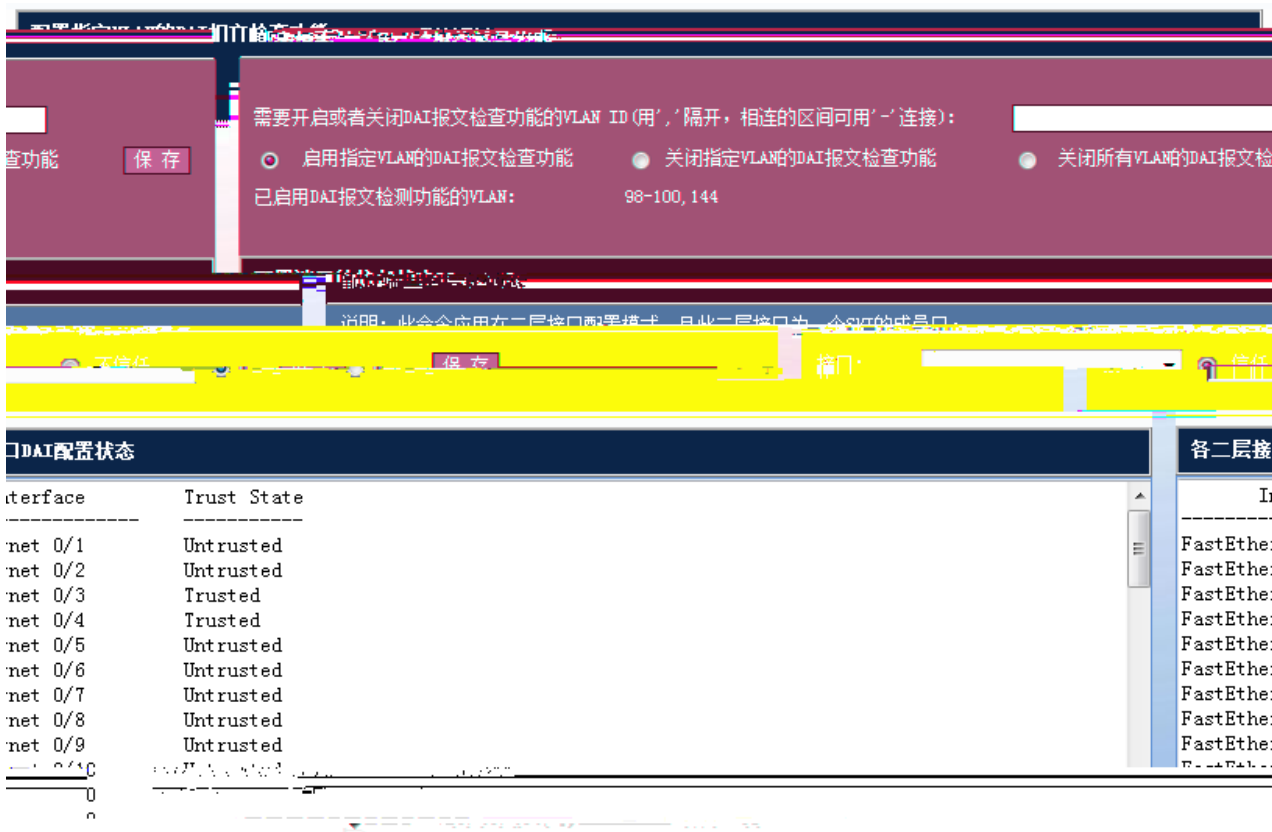
2.3.6 DAI

DAI Dynamic ARP Inspection ARP ARP

 arp

DAI

DAI



45 DAI

1

```

VLAN 100 DAI
VLAN 100 DAI
vlan-id 100 ARP DAI
DAI VLAN ID VLAN
VLAN DAI
    
```

DAI

2.3.7 CPP

CPP

配置报文的带宽和优先级

报文类型: [恢复默认配置](#)

带宽: (1-4096) [保存](#) 优先级: 0

[保存](#) [查看](#)

查看管理板/单机/堆叠系统的接收报文的统计信息: [查看](#)

查看线卡接收报文的统计信息: (2-8) [查看](#)

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
tunnel-bpdu	180	6
ipv4-icmp-local	1600	6
lldp	180	5
lldp_cdp	180	5
cfm-pdu	180	3

46 CPP

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

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
igmp	0	0	0
l2tp	0	0	0
lldp	0	0	0
llnrp	0	0	0
ospf	0	0	0
rip	0	0	0
ripng	0	0	0
stp	0	0	0
stpv2	0	0	0
stpv3	0	0	0
stpv3v1	0	0	0
stpv3v2	0	0	0
stpv3v3	0	0	0
stpv3v4	0	0	0
stpv3v5	0	0	0
stpv3v6	0	0	0
stpv3v7	0	0	0
stpv3v8	0	0	0
stpv3v9	0	0	0
stpv3v10	0	0	0
stpv3v11	0	0	0
stpv3v12	0	0	0
stpv3v13	0	0	0
stpv3v14	0	0	0
stpv3v15	0	0	0
stpv3v16	0	0	0
stpv3v17	0	0	0
stpv3v18	0	0	0
stpv3v19	0	0	0
stpv3v20	0	0	0
stpv3v21	0	0	0
stpv3v22	0	0	0
stpv3v23	0	0	0
stpv3v24	0	0	0
stpv3v25	0	0	0
stpv3v26	0	0	0
stpv3v27	0	0	0
stpv3v28	0	0	0
stpv3v29	0	0	0
stpv3v30	0	0	0
stpv3v31	0	0	0
stpv3v32	0	0	0
stpv3v33	0	0	0
stpv3v34	0	0	0
stpv3v35	0	0	0
stpv3v36	0	0	0
stpv3v37	0	0	0
stpv3v38	0	0	0
stpv3v39	0	0	0
stpv3v40	0	0	0
stpv3v41	0	0	0
stpv3v42	0	0	0
stpv3v43	0	0	0
stpv3v44	0	0	0
stpv3v45	0	0	0
stpv3v46	0	0	0
stpv3v47	0	0	0
stpv3v48	0	0	0
stpv3v49	0	0	0
stpv3v50	0	0	0
stpv3v51	0	0	0
stpv3v52	0	0	0
stpv3v53	0	0	0
stpv3v54	0	0	0
stpv3v55	0	0	0
stpv3v56	0	0	0
stpv3v57	0	0	0
stpv3v58	0	0	0
stpv3v59	0	0	0
stpv3v60	0	0	0
stpv3v61	0	0	0
stpv3v62	0	0	0
stpv3v63	0	0	0
stpv3v64	0	0	0
stpv3v65	0	0	0
stpv3v66	0	0	0
stpv3v67	0	0	0
stpv3v68	0	0	0
stpv3v69	0	0	0
stpv3v70	0	0	0
stpv3v71	0	0	0
stpv3v72	0	0	0
stpv3v73	0	0	0
stpv3v74	0	0	0
stpv3v75	0	0	0
stpv3v76	0	0	0
stpv3v77	0	0	0
stpv3v78	0	0	0
stpv3v79	0	0	0
stpv3v80	0	0	0
stpv3v81	0	0	0
stpv3v82	0	0	0
stpv3v83	0	0	0
stpv3v84	0	0	0
stpv3v85	0	0	0
stpv3v86	0	0	0
stpv3v87	0	0	0
stpv3v88	0	0	0
stpv3v89	0	0	0
stpv3v90	0	0	0
stpv3v91	0	0	0
stpv3v92	0	0	0
stpv3v93	0	0	0
stpv3v94	0	0	0
stpv3v95	0	0	0
stpv3v96	0	0	0
stpv3v97	0	0	0
stpv3v98	0	0	0
stpv3v99	0	0	0
stpv3v100	0	0	0

49 / /

2.3.8 RADIUS

RADIUS

1 RADIUS



50 RADIUS



2 RADIUS

Radius服务器 Radius服务器组

AAA参数配置

AAA new-model: 开启 关闭

密钥: 隐藏密钥 保存

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:

正端口: (0-65536) (可选) UMF认证

帐端口: (0-65536) (可选) UMF记

保存

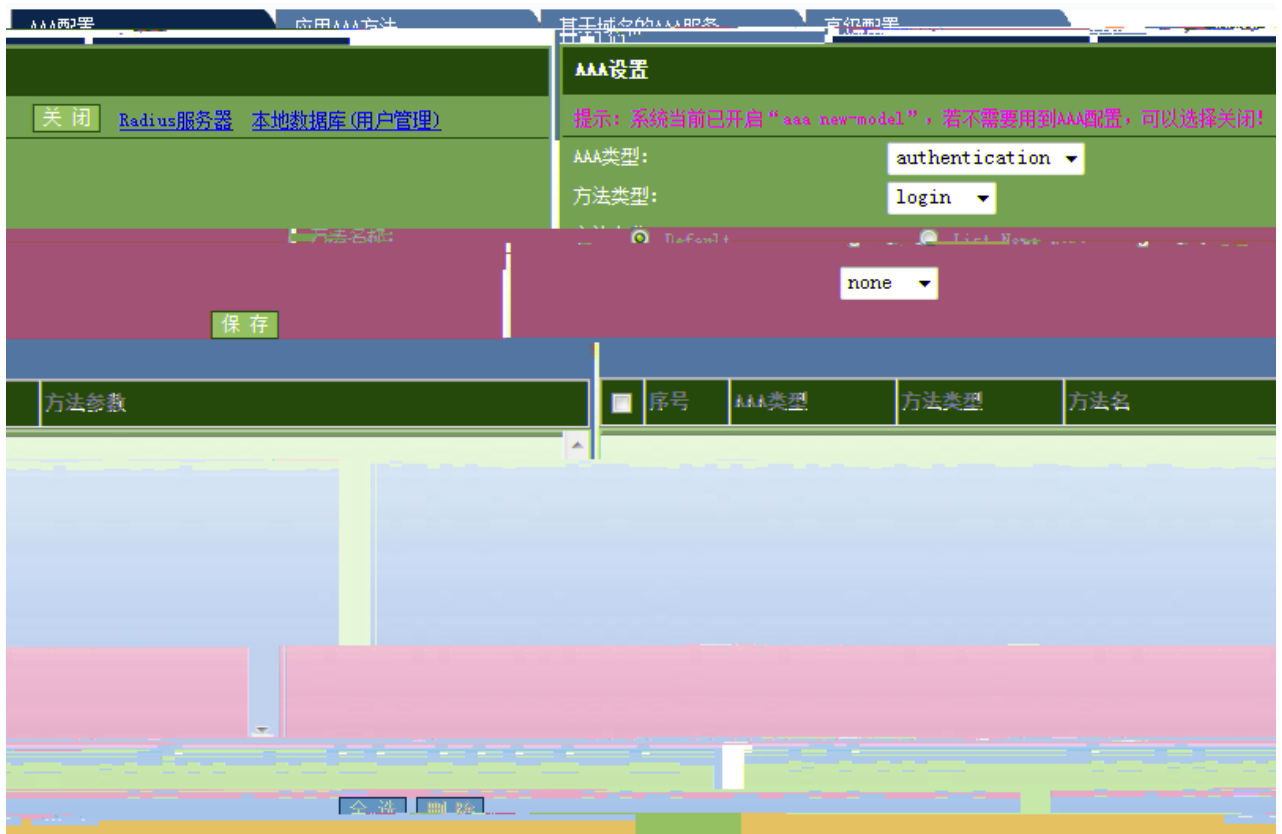
服务器组管理: radius 删除 刷新

```

=====Radius group radius=====
Vrf:not-set
Server:7::1
  Authentication port:1812
  Accounting port:1813
  State:Active
Server:::1
  Authentication port:1812
  
```

192.168.1.100
port:1813
State:Active

51 RADIUS



52 AAA

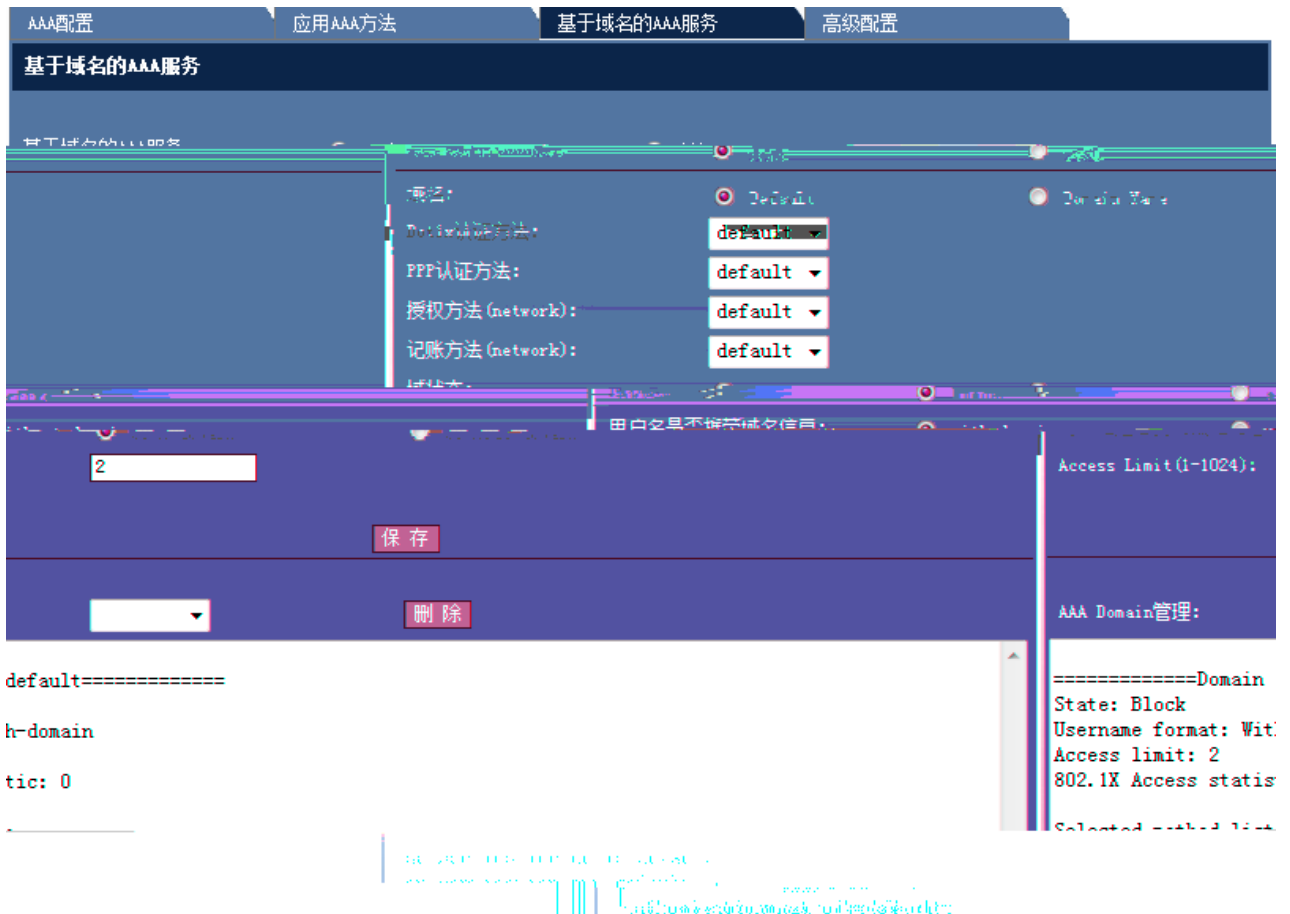
1

AAA

AAA

3

AAA



54

AAA

(network)

AAA

(network)

Dot1x

PPP

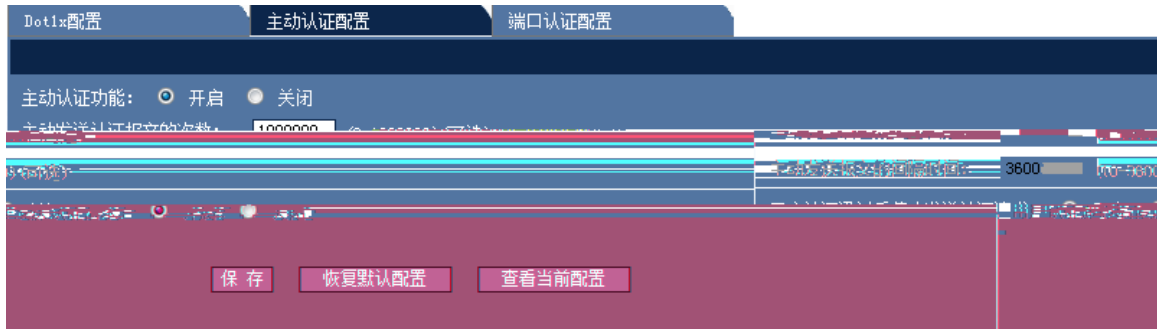
Access Limit

AAA Domain

4 AAA

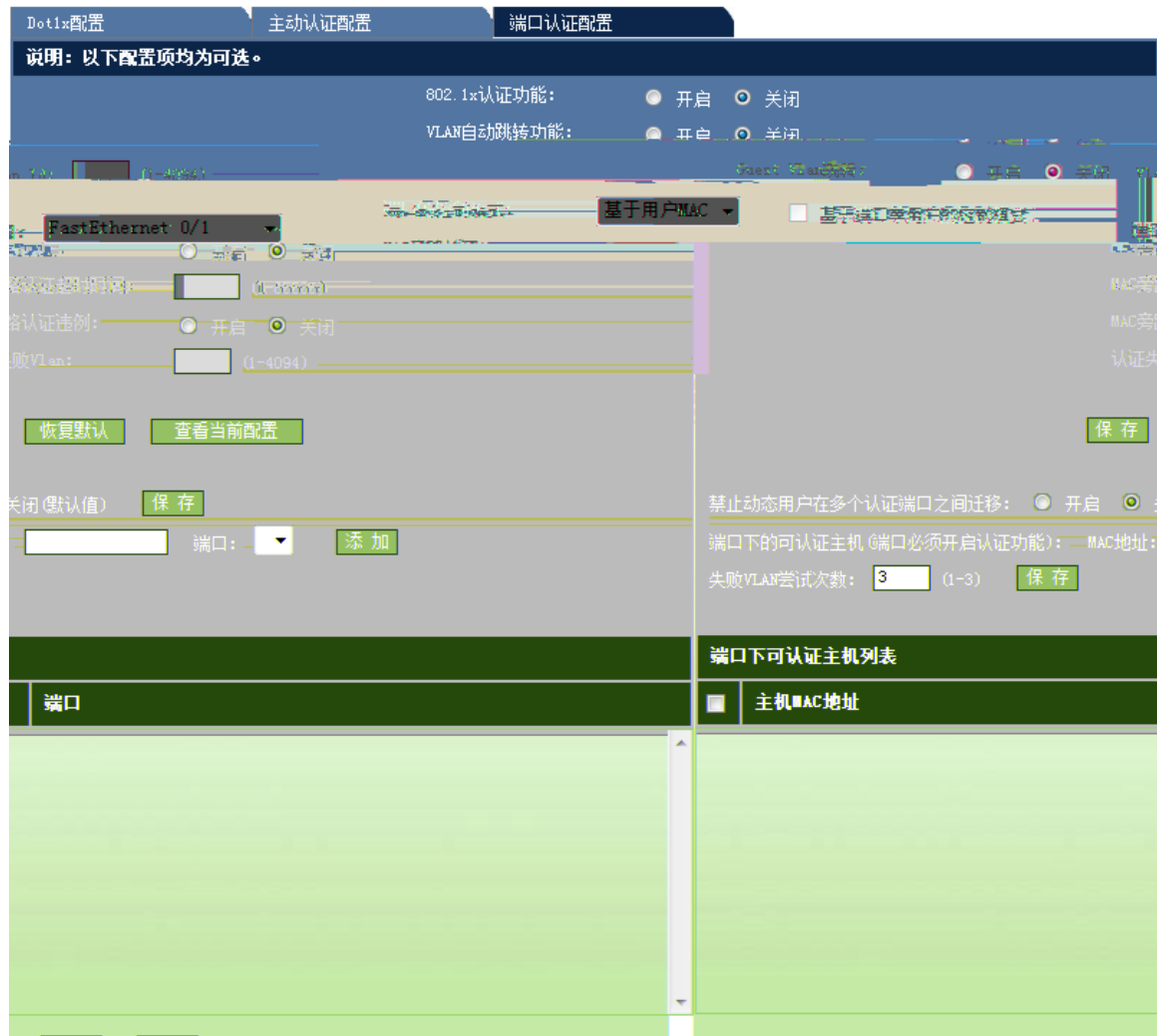
Dot1x

2



57

3



58

Dot1x

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.a805	1	绑定
3	192.168.23.55	001...	1	绑定
4	192.168.23.76	001...	5	绑定
5	192.168.23.76	001...	5	绑定
6	192.168.23.76	001...	5	绑定
7	192.168.23.76	001...	5	绑定

刷新

61 ARP

2.3.12 WEB

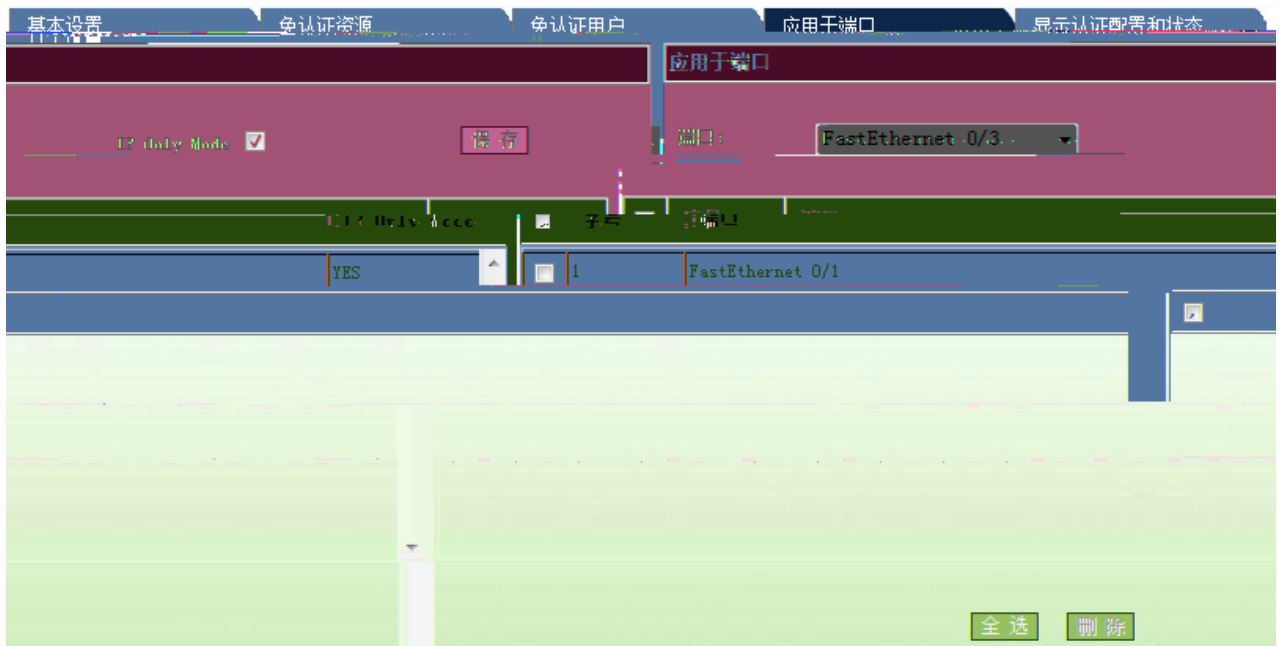
web

web



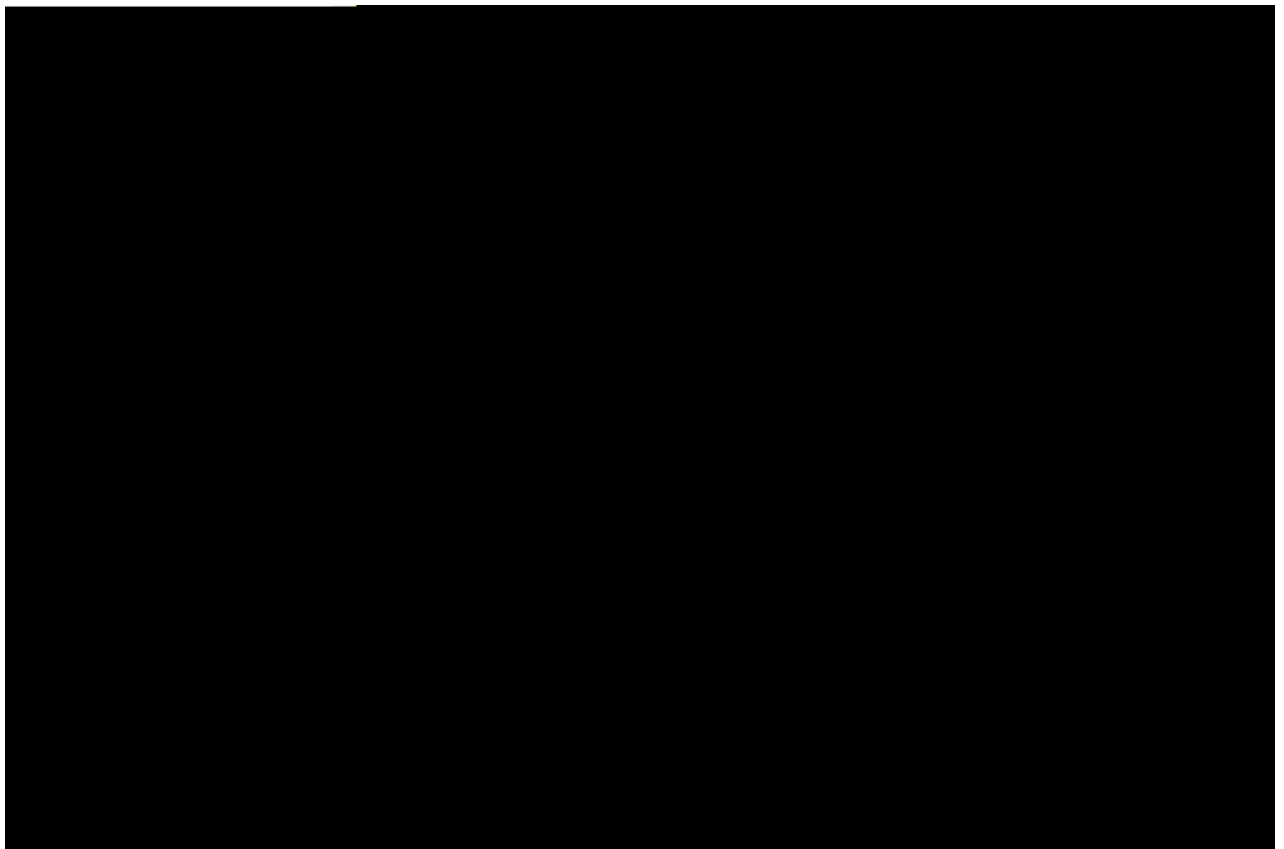


63.



65

5)



66

IP

2.3.13 DHCP Snooping

DHCP Snooping

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。

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
1	FastEthernet 0/1	信任	10000000

全选
删除

67 DHCP Snooping

DHCP Snooping

DHCP Snooping

MAC

2)DHCP Snooping

2.4 QOS

2.4.1



68

ACL

2.4.4

将风暴控制应用于端口 (端口默认开启风暴控制)

端口: FastEthernet 0/2

广播 默认

抑制 suppression_level 20

保存

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

全选 删除

71

2.4.5



72

1)

Sticky Mac

Static

2)



73

Mac

VLAN ID

3)

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

74

Mac IP
VLAN ID MAC Vlan

2.5

2.5.1

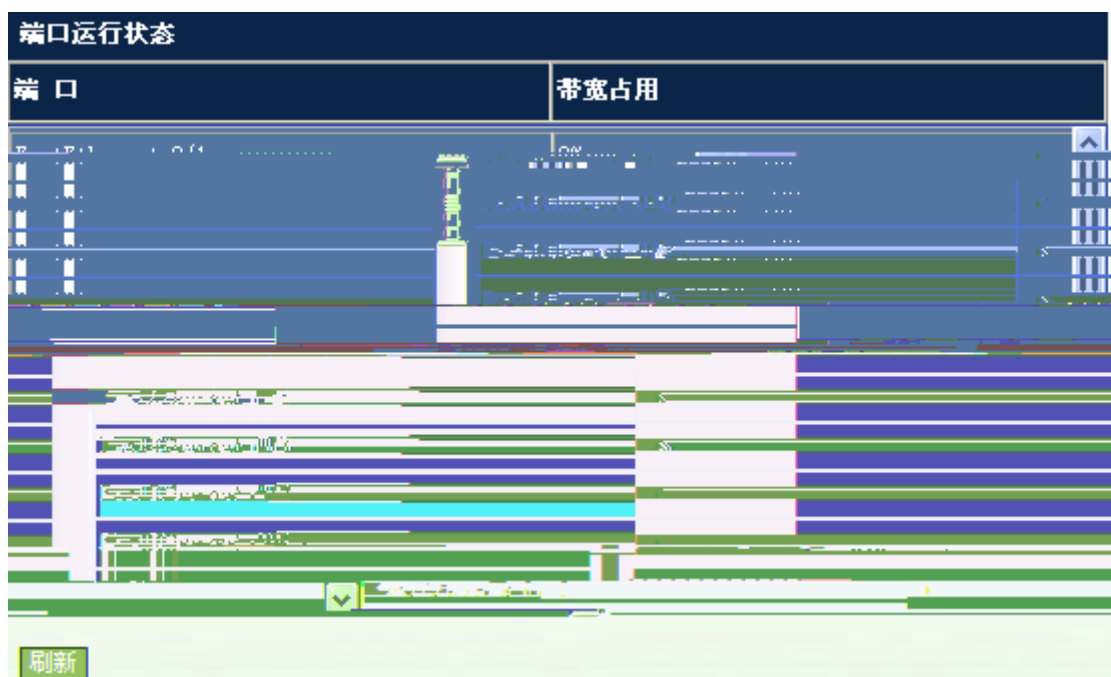
端口状态

端口	名称	状态	速率	模式	速率	
copper	FastEthernet 0/1	down	1	Unknown	Unknown	
copper	FastEthernet 0/2	down	2	Unknown	Unknown	
copper	FastEthernet 0/3	up	1	Full	100%	
copper	FastEthernet 0/4	down	900	Unknown	Unknown	
per	FastEthernet 0/5	down	1	Unknown	Unknown	
per	FastEthernet 0/6	down	1	Unknown	Unknown	
down	Unknown	copper	FastEthernet 0/10	down	1	Unknown

刷新

77

2.5.4



78

2.5.5



端口统计信息

注意：选择端口后，将相应端口的统计信息列表显示在下方。

端口：

输入/输出帧统计

接收多播包数	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	发送包数	发送单播包数	发送多播包数
0	1689	Gi0/1	33198	8950	5508	18740	14043	12012	34
0	0	Gi0/2	0	0	0	0	0	0	0
2157	2146	Gi0/3	6	5	6264	3004	543	2717	0
0	0	Gi0/4	0	0	0	0	0	0	0
34	23	Gi0/5	11	0	217	15	27	175	0
0	0	Gi0/6	0	0	0	0	0	0	0
882792	404167	Gi0/7	69848	408777	3430900	436541	695541	2298818	0
0	0	Gi0/8	0	0	0	0	0	0	0
437082	435647	Gi0/9	37	1398	1719318	685632	191269	842417	0
0	0	Gi0/10	0	0	0	0	0	0	0
856226	850552	Gi0/11	149	5525	4080490	958886	754472	2367132	0
0	0	Gi0/12	0	0	0	0	0	0	0
0	0	Gi0/13	0	0	0	0	0	0	0
0	0	Gi0/14	0	0	0	0	0	0	0
5557815	1423231	Gi0/15	935630	3198954	1060302	1051703	213	8386	0
0	0	Gi0/16	0	0	0	0	0	0	0

79

2.5.6

```

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
  Sysname log messages: disable
  Count log messages: disable
  Trap logging: level informational, 587 message lines
  Log Buffer (Total 4096 Bytes): have written 4096. Overw
logged, 0 fail
ritten 2533
*Feb 28 06:20:49: %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.
*Feb 28 06:53:54: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 07:03:55: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 07:13:57: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 07:23:59: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 07:34:00: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 07:44:01: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 07:54:03: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 08:04:04: %ARPGUARD-4-SCAN: ARP scan was detected.
*Feb 28 08:14:06: %ARPGUARD-4-SCAN: ARP scan was detected.

```

80

2.6

2.6.1 Ping

Ping

IP

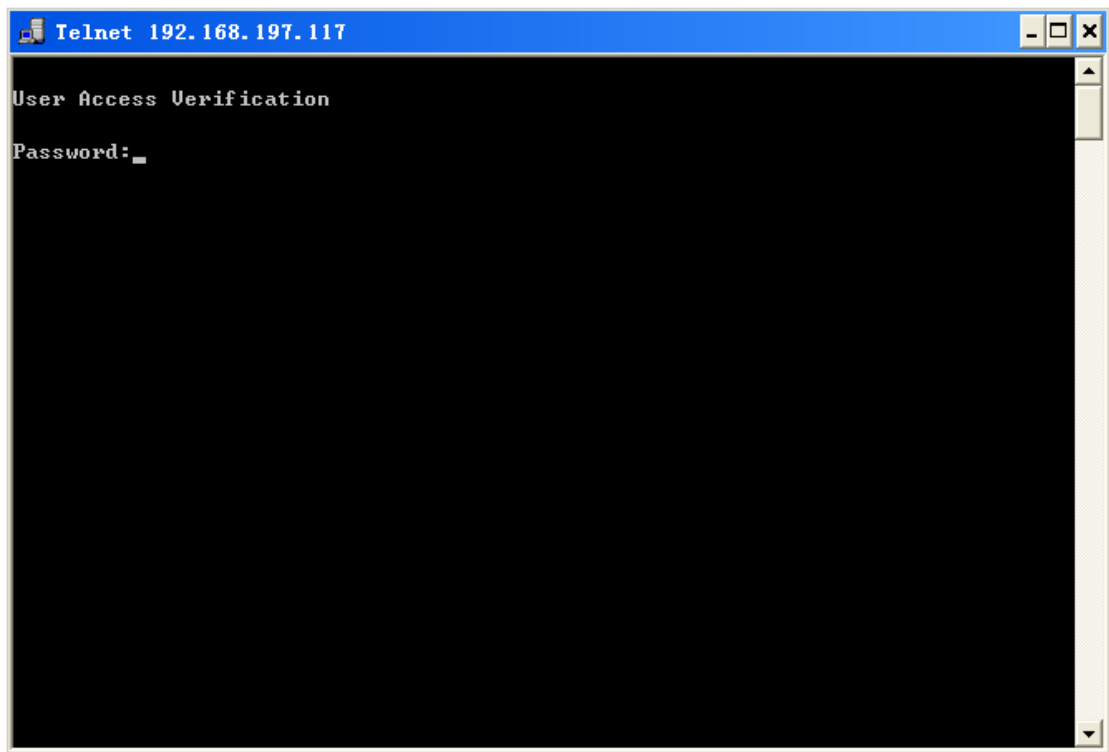
IP

Ping

2.6.2 Telnet

Telnet

Telnet



82 Telnet

PC Telnet Telnet PC Telnet

2.6.3



85

2.6.4

The image shows two screenshots of a network device's web management interface. The top screenshot is titled "修改Enable口令" (Modify Enable Password). It contains a green sidebar with a warning message: "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。" (Note: If you set a new Enable password, use the new password to log in again after the setting). To the right, there are two input fields: "新口令" (New Password) and "确认新口令" (Confirm New Password), each followed by a colon. Below these fields is a "保存" (Save) button. The bottom screenshot is titled "修改Telnet登录口令" (Modify Telnet Login Password). It features a similar green sidebar and a single "新口令" (New Password) input field with a colon. Below this field is another "保存" (Save) button.

86

- 1) Enable
Enable



87

- 2) Telnet
Telnet

8080

IP

192.168.1.1

:8080

2.6.7

系统升级

注意：请确认TFTP服务器已启用！

源文件名：

目标文件名：

TFTP 服务器 IP：

文件传输信息：

系统升级过程需要若干分钟,请耐心等待...

90

TFTP



