

WEB

RG-S6000E

S6000E_RGOS11.4(1)B2

V .0

copyright © 2016





1 Eweb

WEB IE WEB

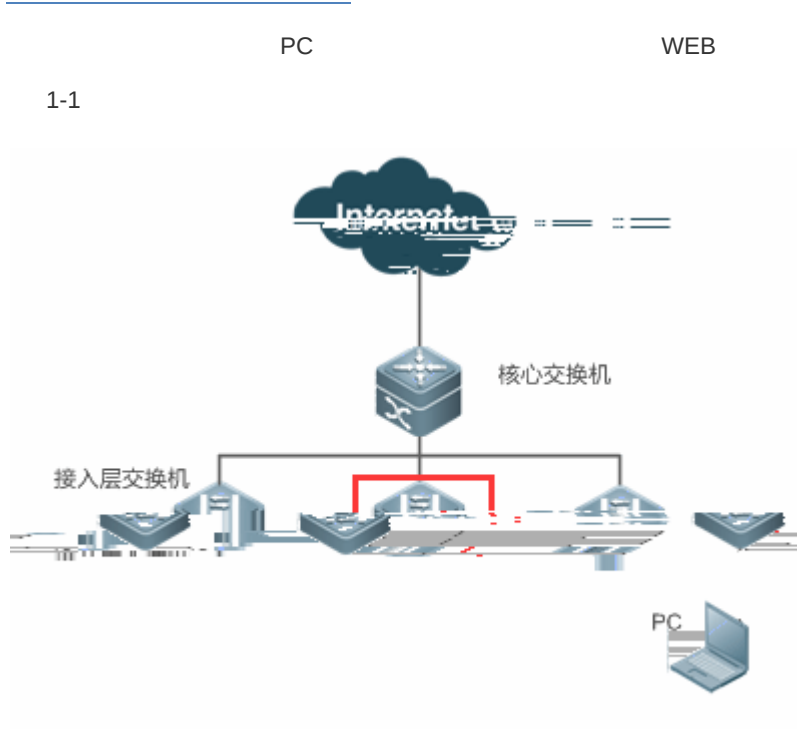
WEB WEB WEB WEB IE WEB

WEB

✓ S6000E

<u>WEB</u>	WEB

1.2.1 WEB



PC ping



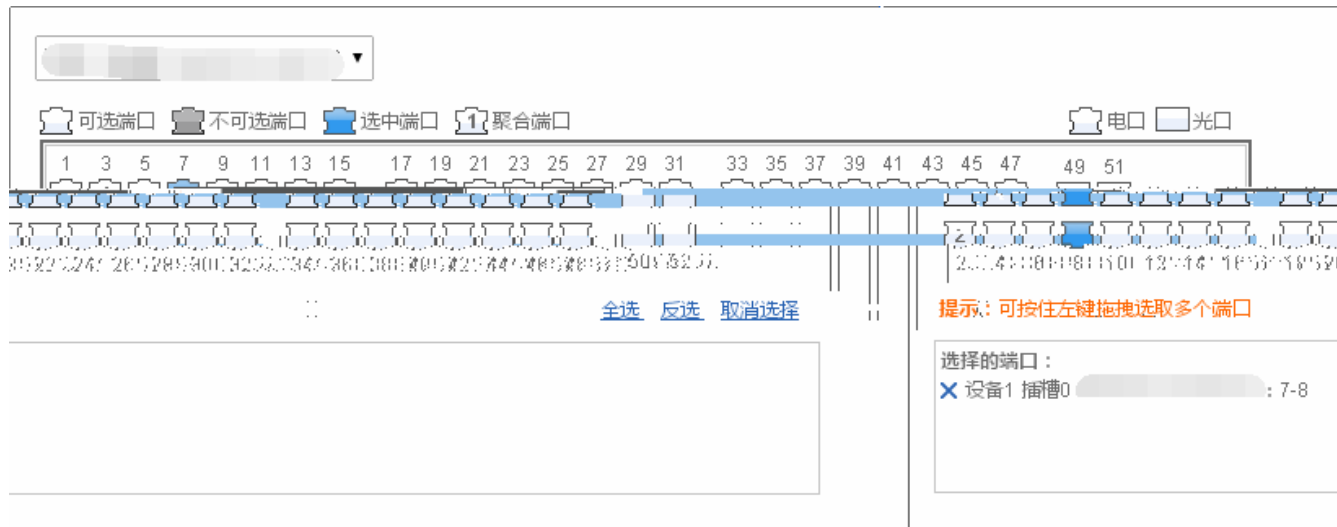
RG交换机

极简网络，新一代交换机

登录

[忘记密码?](#)

[English ▶](#)



WEB

VLAN	VLAN Trunk
MAC	
	RLDP
IGMP	IGMP Snooping
DHCP	DHCP
	web
DHCP Snooping	DHCP Snooping
ARP	ARP ARP DAI ARP
IP Source Guard	

DHCP

“ ”

VLAN

1.3.2.1

1-5



1.3.2.2 VLAN

VLAN “ VLAN ” “ Trunk ”

➤ VLAN

VLAN

1-6 VLAN

VLAN设置

Trunk口设置

+批量添加VLAN

+添加VLAN

X删除选中VLAN

	VLAN ID	VLAN名称	IPv4 IP	掩码	端口	操作
☐	1	VLAN0001	172.18.124.73	255.255.255.0	Gi0/1-10, Gi0/13-16, Gi0/25-26 Ag2, Ag7, Ag25	编辑
☐	2	VLAN0002			Gi0/13-14	编辑 删除
☐	4	HHHHfffjh			Gi0/13-14	编辑 删除
☐	5	VLAN0005			Gi0/13-14	编辑 删除
		Gi0/13-14				删除
		Gi0/13-14				删除
		Gi0/13-14				删除
		Gi0/13-14				删除
255.255.255.0		Gi0/13-14				删除
		Gi0/13-14				删除

显示 10 条 共 14 条

- VLAN

VLAN VLAN ID “ ” “ ” VLAN
- VLAN

“ VLAN ” < > VLAN < >

“ ”
- VLAN

1 “ VLAN ” “ VLAN ”

2 “ VLAN ” < > “ vlan ” “ ”

VLAN 1 VLAN

VLAN1 VLAN

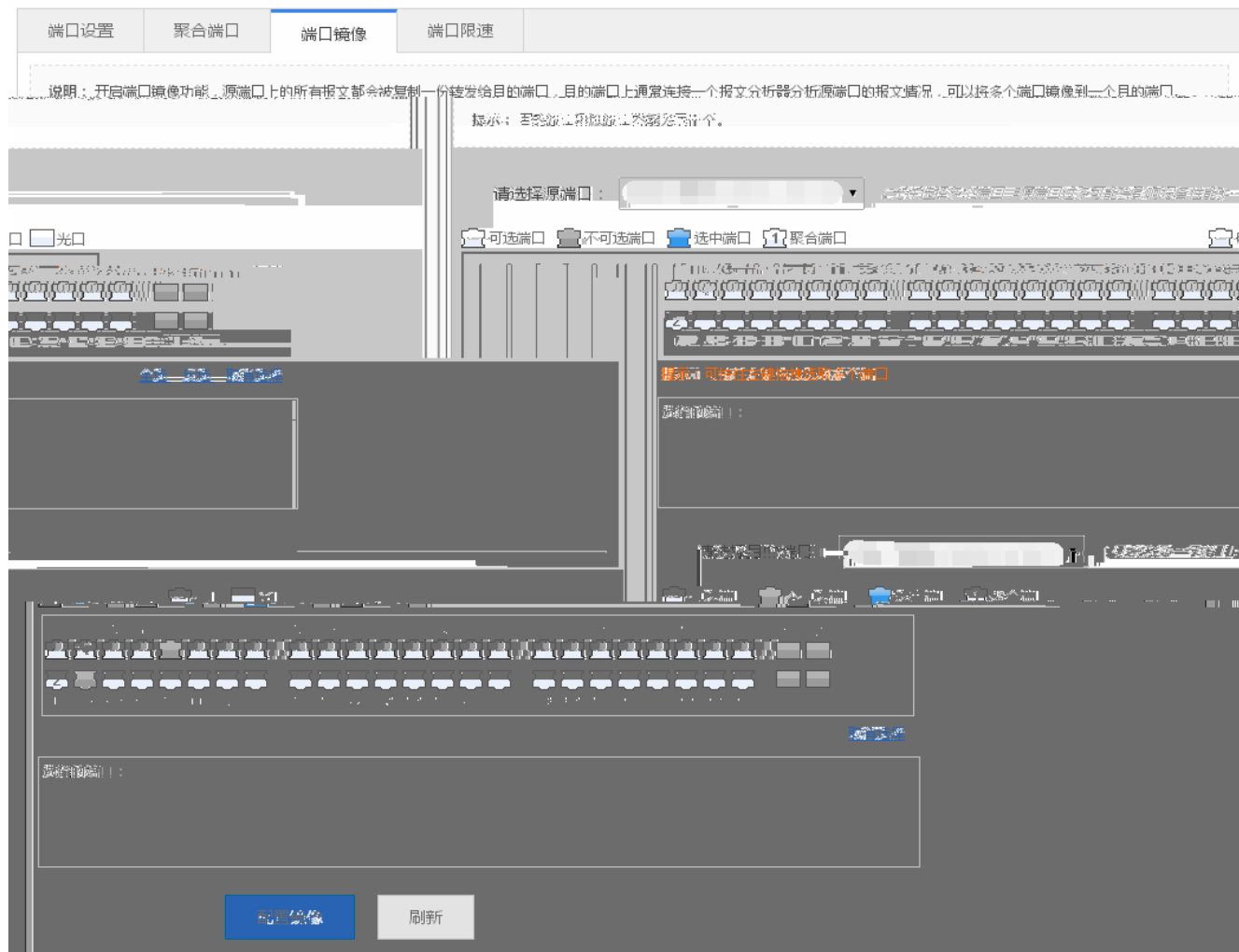
Trunk

Trunk

1-7 Trunk



1-10



web



1-11

端口设置

聚合端口

端口镜像

端口限速

端口安全

端口转发

端口管理

+ 批量配置限速端口

✕ 批量删除限速端口

操作	☐	端口	输入速率(Kbps)	输出速率(Kbps)	
编辑 删除	☐	Gi0/9	102400	102400	

显示

10

条共1条

首页

上一页

下一页

●

“ ” “ ”

●

“ ” < > < >

“ ”

●

1 “ ” “ ”

2 “ ” < > “ ” “ ”

1.3.2.4

1-12

系统重启

说明：点击重启按钮将使设备重新启动，重启过程需要2分钟左右的时间，请耐心等待，设备重启后将会自动刷新页面。

重启设备

< > “ ” < >

1-14

静态地址设置

过滤地址设置

说明：交换机在转发数据时，需要根据MAC地址表来做出相应转发，当在配置的VLAN中接受到源地址或目的地址为配置的MAC地址时，将丢弃此报文，不进行转发。应用场景如某个用户发起ARP攻击时，可以将其配置为过滤地址，防止攻击。

+ 添加过滤地址

✕ 删除过滤地址

☐	MAC地址	VLAN ID	操作
☐	0002.0002.0003	4	编辑 删除

显示: 10 条 共1条

◀ 首页 < 上一页 1 下一页 > 末页 ▶

1

确定

MAC

VLAN ID

" "

" "

" "

< >

< >

" "

" "

2

" "

< >

" "

" "

1.3.3.2

" "

1-15

路由管理

说明：路由选路 分为 主路由和备份路由，当主路由不能生效，就会走备份路由，备份路由按照配置的级别优先级来走，备份路由1 的优先级比备份路由2 的优先级来的高。

+ 添加静态路由

+ 添加默认路由

✕ 删除选中路由

☐	目的网段	目的网段掩码	下一跳地址	出口	路由选路	类型	操作
无记录信息							

显示: 10 条 共0条

⏮ 首页

◀ 上一页

下一页 ▶

末页 ⏭

1

确定

IP

“ ” “ ”

“ ” < > < > “ ”

”

1 “ ” “ ”

2 “ ” < > “ ” “ ”

IP

“ ” “ ”

1

2

1.3.3.3

“ ” RLDP

1-16

1-17

生成树全局设置

生成树端口设置

RLDP设置

三 全局设置

生成树开关：

ON

优先级：

8

范围(0-15)，默认8握手时间：

2

范围(1-10)秒，默认2

老化时间：

20

范围(1-40)秒，默认20转发延迟：

30

范围(1-40)秒，默认30

树模式：

MSTP

保存设置

三 MST 设置

+ 添加实例

× 删除选中实例

优先级	操作	实例值	VLAN
8	默认实例，不可编辑	0	ALL

“ MSTP ” MST

●

VLAN

“ ” “ ”

●

“ ” “ ”

●

1 “ ” “ ”

2 “ ” “ ”

0

1-17

生成树全局设置

生成树端口设置

RLDP设置

RLDP全局设置

说明：RLDP可以方便快速地检测出以太网设备的链路故障,只有全局的RLDP打开,端口RLDP才能运行。

RLDP开关：

ON

探测间隔：

3

范围(2-15s)

探测次数：

2

范围(2-10)

恢复周期：

300

范围(30-86400s)

保存设置

端口RLDP设置

说明：RLDP分为全局RLDP和端口RLDP。全局RLDP打开后，端口RLDP才能运行。端口RLDP打开后，可以检测出该端口的链路故障。当检测到链路故障时，端口RLDP会自动关闭该端口，防止网络环路。当链路恢复正常后，端口RLDP会自动恢复该端口。

增加RLDP检测端口

删除RLDP检测端口

清除RLDP检测端口

重置RLDP检测端口

保存RLDP检测端口

取消RLDP检测端口

检测类型	故障处理	操作
无记录信息		

显示 10 条共0条

1 RLDP

RLDPRLDP<>“

”

2 RLDP

●RLDP

“ ” “ ” “ ” “ ” RLDP

“ RLDP ”

●RLDP

“ RLDP ” < > RLDP

< > “ ”

●

“ RLDP ” “ RLDP ”

1.3.3.4 IGMP

IGMP

1-18 IGMP Snooping

[IGMP Snooping](#)

说明：在二层设备下，组播帧是作为广播转发的，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。

+ 添加组策略

✕ 删除选中组策略

IGMP Snooping开关：

ON

	组策略标识	组播地址	策略动作	策略应用端口	操作
无记录信息					

显示: 10 条共0条

◀ 首页

◀ 上一页

下一页 ▶

末页 ▶▶

1

确定



DHCP 中继

说明：DHCP中继可以实现不同子网之间的IP分配，相当于一个中转站，它将收到的客户端请求报文转发给指定的DHCP服务器，并将收到的服务器响应报文转发给客户端。

三 DHCP IPv4中继配置

DHCP中继开关：

ON

DHCP服务器地址：

+ 增加DHCP服务器

保存设置

DHCP

DHCP

1.3.3.6

“ ”

web

↘

web

web

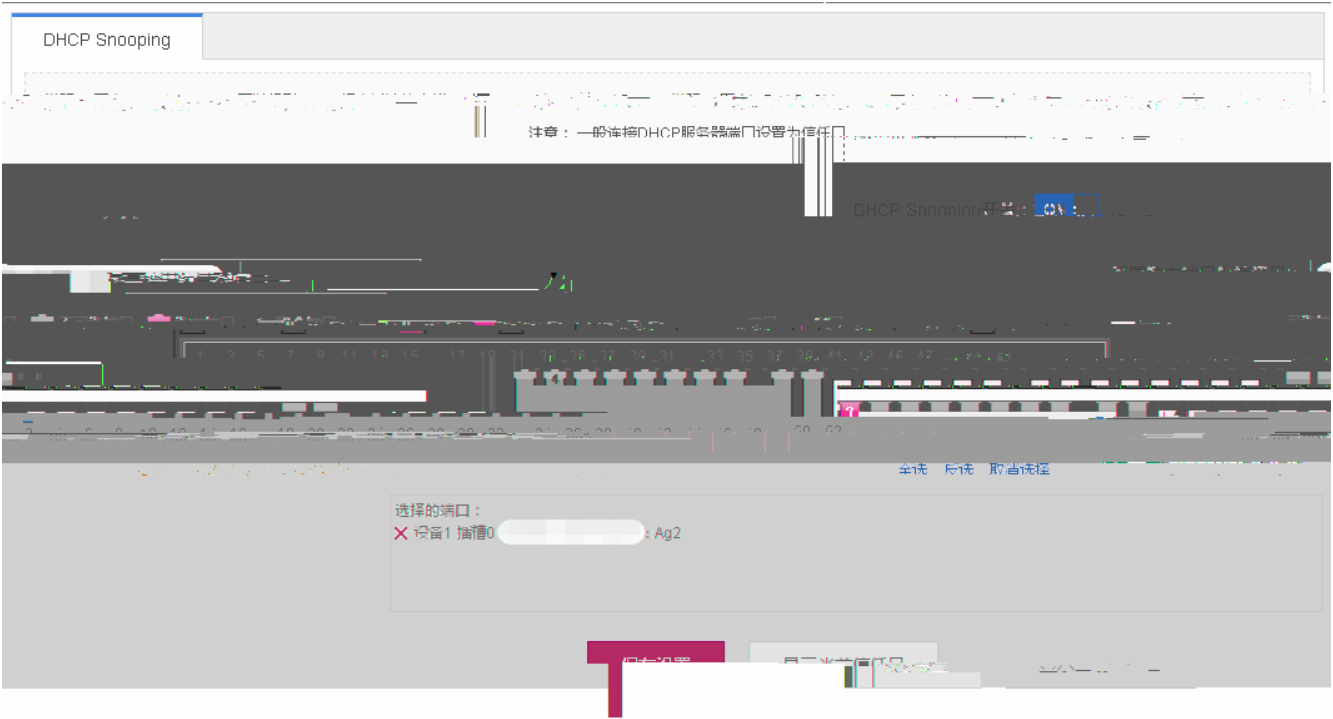
1-20

web

1-22

NFPP

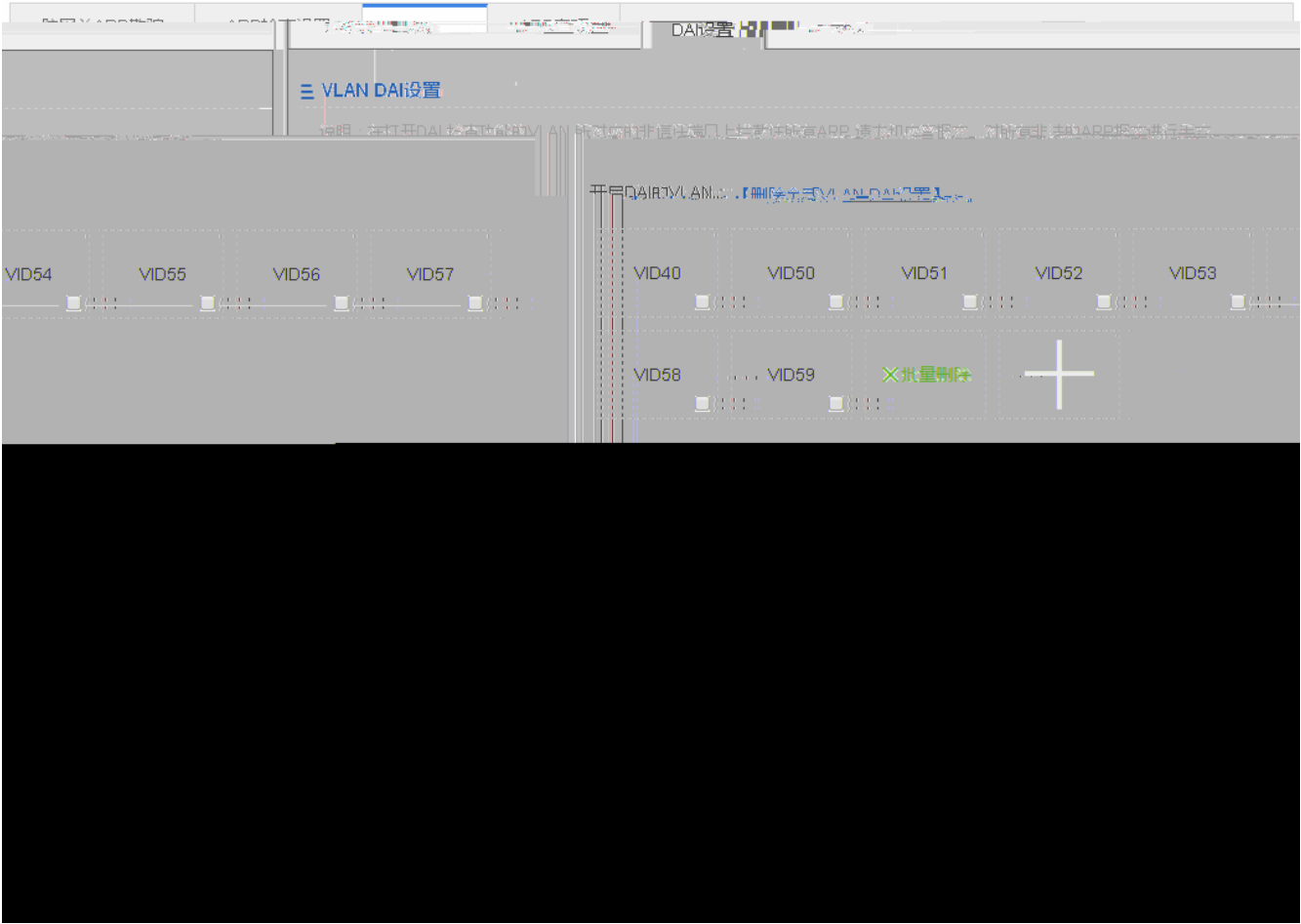
1-22 DHCP Snooping



DHCP SERVER DHCP DHCP SERVER
DHCP < >

1.3.4.2 ARP

“ ARP ” ARP ARP DAI ARP
↓ ARP
1-23 ARP



1 VLAN DAI

DAI VLAN

2 DAI

DAI



DAI

<

DAI

>

DAI



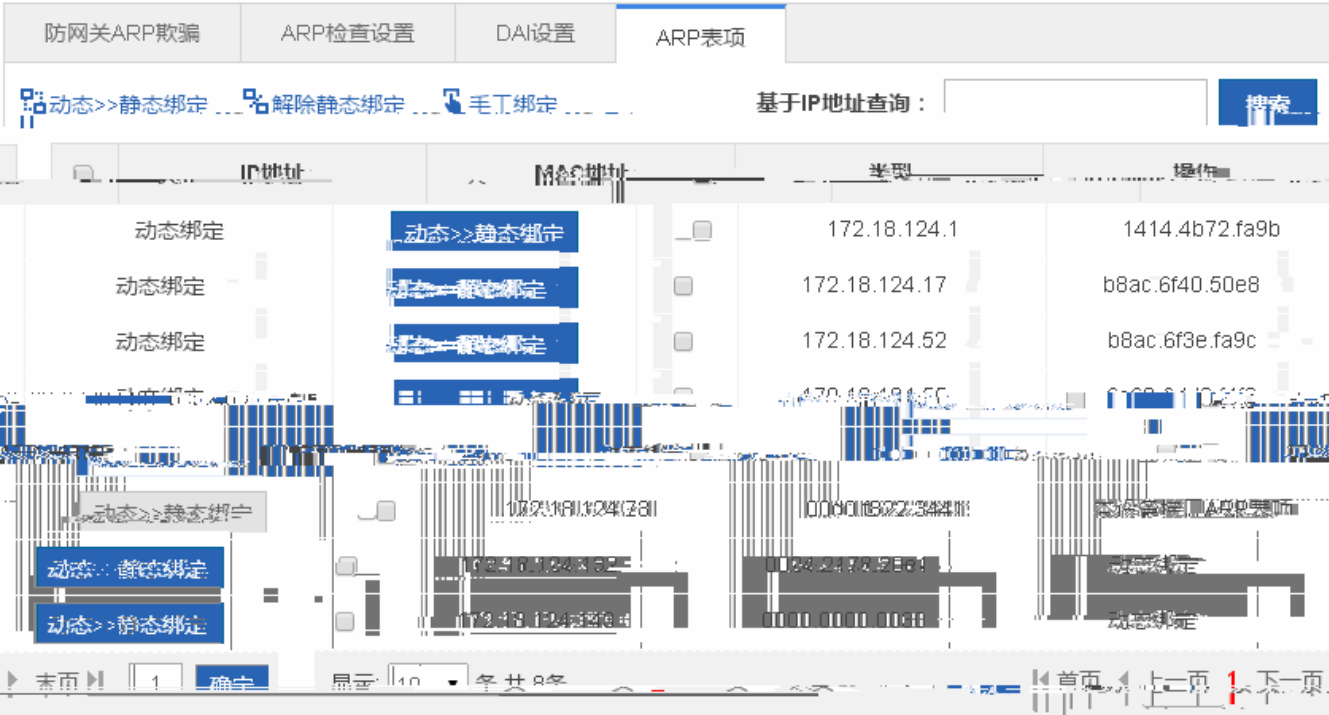
DHCP Sn ooping

ARP



ARP

1-26 ARP



●

>>

1

“ ARP ”

2

“ ARP ”

<

>

“ ”

●

1

“ ARP ”

2

“ ARP ”

<

>

“ ”

●

IP

MAC

“ ”

“ ”

“ ARP ”

1.3.4.3 IP Source Guard

“ IP Source Guard ”

↓ 。 ”



- IP Source Guard
IP Source Guard “ ” “ ” IP Source Guard
- IP Source Guard
“ IP Source Guard ” < > IP Source Guard
< > “ ”
- IP Source Guard
1 “ IP Source Guard ” “ IP Source Guard ”
2 “ IP Source Guard ” < > “ ” “ ”

	MAC	IP	VLAN ID	"	"	"	"
	"	"	<	>			<
	>	"	"				
1	"	"	"	"	"		
2	"	"	<	>	"	?"	"

1.3.4.4



1-29

基本设置

安全绑定

说明：一般适用于希望控制端口下接入用户的IP和MAC是指定的合法用户，或者希望使用者能够在固定端口下上网而不能随意移动，变换IP/MAC或

+ 添加安全口

✕ 删除选中的安全口

端口	限定MAC数	老化时间	违例处理方式	操作
无记录信息				

◀ 首页

◀ 上一页

下一页 ▶

▶ 末页 ▶▶

1

确定

显示: 10 ▼ 条 共0条

	IP	"	"	"	"
	"	"	<	>	<
	>	"	"		
1	"	"	"	"	

2

“ ”

< >

“ ”

“ ”



1-30

基本设置

安全绑定

说明：设定端口安全绑定地址，绑定IP或IP+MAC，用来限制必须符合绑定的以端口安全地址为源MAC地址的报文才能进入交换机通信。

+ 添加安全绑定地址

✕ 删除选中的安全绑定地址

☐	端口	IP地址	MAC地址	VLAN ID	操作
无记录信息					

显示 10 条, 共0条

首页 上一页 下一页 末页

1/1

确定

●

IP

“ ” “ ”

●

“ ”

< >

<

>

“ ”

●

1

“ ”

“ ”

2

“ ”

< >

“ ”

“ ”

1.3.4.5 NFPP

NFPP

1-31 NFPP

NFPP

ARP防攻击：☐ 开启ARP防攻击，防止大量非法ARP报文攻击设备。设备每秒处理的ARP报文 不超过4个。
[【ARP防攻击列表】](#)

IP防扫描：☐ 开启IP防扫描，防止大量非法IP扫描设备。设备每秒处理的IP扫描报文 不超过4个。
[【IP防扫描列表】](#)

ICMP防攻击：☒ 开启ICMP防攻击，防止大量非法ICMP占用带宽和CPU资源，设备每秒处理的ICMP报文 不超过4个。
[【ICMP防攻击列表】](#)

DHCPv4防攻击：☐ 开启DHCPv4防攻击，防止DHCPv4被恶意请求使地址池耗尽，导致合法用户获取不到IPv4地址。
[【DHCPv4防攻击列表】](#)

DHCPv6防攻击：☒ 开启DHCPv6防攻击，防止DHCPv6被恶意请求使地址池耗尽，导致合法用户获取不到IPv6地址。
[【DHCPv6防攻击列表】](#)

ND防攻击：☒ 开启ND防攻击，防止“邻居发现”报文占用带宽，每秒处理报文 不超过15个。

查看防攻击日志：[【本地防攻击日志】](#)

保存设置 恢复默认设置

1.3.4.6

1-32

风暴控制

+ 添加风暴控制端口 X 删除选中的风暴控制端口

☐	端口	广播	组播	单播	操作
☐	Gi0/16	90%	-	-	编辑 删除

显示 10 条 共1条

◀ 首页 1 下一页 ▶ 末页 1 确定

“ ”

< >

<

> “ ”

“ ”

●

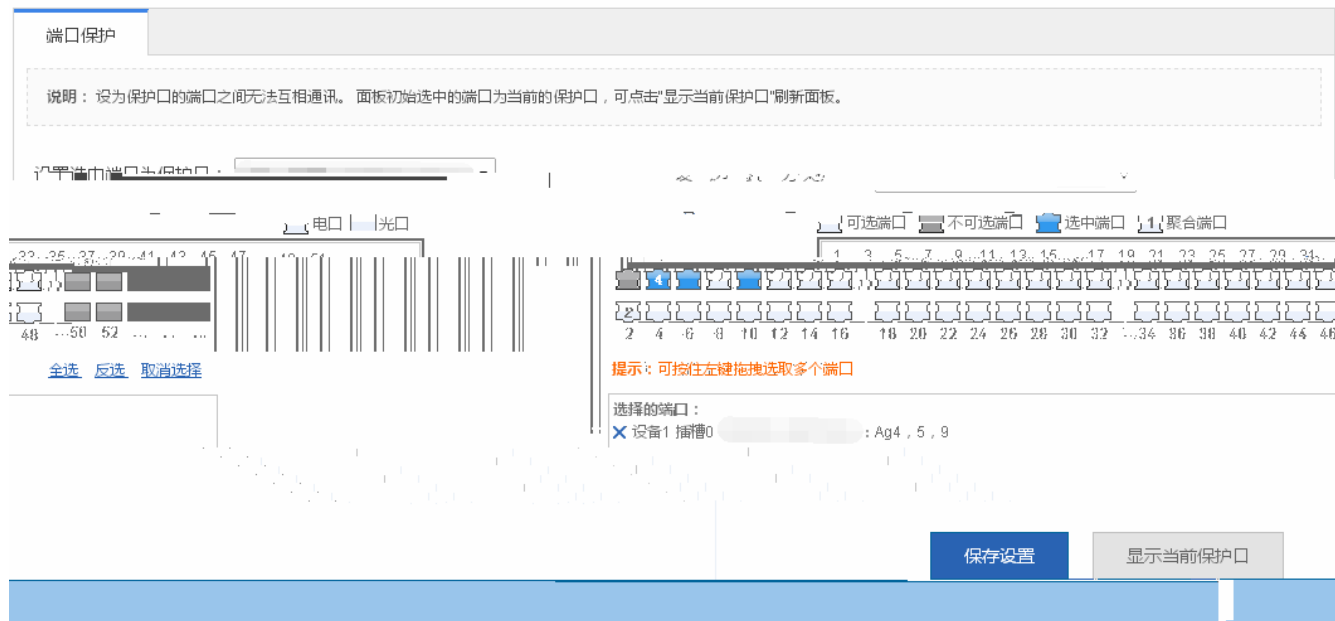
1 “ ” “ ”

2 “ ” < > “ ” “ ”

1.3.5

1.3.5.1

1-33



1.3.5.2 DHCP

“ DHCP ” DHCP ES224GT

↙ DHCP

DHCP

1-34 DHCP

●

“ ” “ ”

●

 $\angle$ $\triangleright$

●

“ ”

66 33



●

IP

IP

IP ”

ACL

1-36

● 1968 ACL " ACL " ACL " " " ACL

● 1970 ACL ACL ACL " ACL " " "

● 1972 ACL ACL IP " " " " ACL

● 1980 ACL " ACL " < > ACL <

> " "

● 1992 ACL

1 " ACL " " "

2 " ACL " < > " " " "

- ACL
ACL “ ” “ ” ACL
“ ACL ” < > ACL <
> “ ”
- ACL
“ ACL ” “ ”

ACL

ACL

1-39 ACL

ACL时间

应用ACL

应用端口

✕删除ACL应用端口

+添加ACL

操作	ACL	应用端口	过滤方向
编辑 删除	test	Gi0/24	in
100% 100%	test	Gi0/24	in

◀ 首页

◀ 上一页

1

下一页 ▶

末页 ▶

1

显示

10

条共2条

- ACL
ACL ACL “ ” “ ” ACL
- ACL
“ ACL ” < > ACL <
> “ ”
- ACL
1 “ ACL ” “ ACL ”
2 “ ACL ” < > “ ” “ ”

1.3.5.4 QOS



1-40

分类设置

策略设置

流设置

说明：分类设置采用ACL的匹配规则识别出符合某类特征的数据流，并对该数据流进行标记。

+ 添加分类

✕ 删除选中的分类

☐	分类名	ACL	操作
☐	testclass	test	编辑 删除

显示: 10 条 共1条

⏮ 首页

◀ 上一页

1

下一页 ▶

末页 ⏭

1

确定

ACL

“ ”

< >

< >

“ ”

1 “ ” “ ”

2 “ ” < > “ ” “ ”

1-41

分类设置

策略设置

流设置

说明：策略动作发生在数据流分类完成后，它用于约束被分类的数据流所占用的传输带宽。

添加策略

删除策略

+ 添加策略规则

✕ 删除选中规则

策略列表: dsaff

带宽(Kbps)	突发流量(KBytes)	带宽超出处理	操作
无记录信息			

⏮ 首页 ◀ 上一页 下一页 ▶ 末页 ⏭ 1 确定

☐

类名

显示: 10 条 共0条

“ ” “ ”

分类设置

策略设置

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（同一端口的输入输出流必须对应相同的信任模式，可以对应不同的策略）。

+ 添加应用策略端口

✕ 删除选中的应用策略端口

☐	端口	方向	策略名	信任模式	操作
无记录信息					

共0条

◀ 首页

◀ 上一页

下一页 ▶

末页 ▶

1

确定

显示: 10 条

" " " " " " " " " " SNMP " " DNS "

	SNMP	DNS
1. Network	• Network • Hosts • Ports • Services • Configuration • Performance • Security • Availability • Logging • Alerting • Reporting • Monitoring • Configuration • Performance • Security • Availability • Logging • Alerting • Reporting • Monitoring	• Network • Hosts • Ports • Services • Configuration • Performance • Security • Availability • Logging • Alerting • Reporting • Monitoring • Configuration • Performance • Security • Availability • Logging • Alerting • Reporting • Monitoring

IP	IP	web

系统时间

修改密码

恢复出厂设置

增强功能

SNMP

DNS

Web网管密码修改

用户名：admin

原密码：

*

新密码：

*

确认密码：

*

保存设置

Telnet密码修改(修改telnet和enable的密码)

用户名：admin

新密码：

*

确认密码：

*

保存设置

● Web

Web

“ ”

< >

web

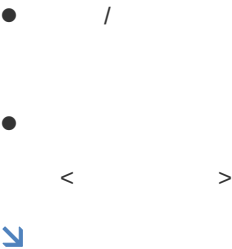
enable

● Telnet

telent

1-45

1-42



1-46

系统时间	修改密码	恢复出厂设置	增强功能	SNMP	DNS	
------	------	--------	------	------	-----	--

≡ 基本信息

WEB访问端口：

80

*(范围80,1025-65535)

登录超时：

10分钟

▼

设备位置：

设备名称

保存设置

WEB

< > “ ”

⌵ SNMP

SNMP

1-47 SNMP

SNMP

SNMP

Trap

< > “ ”

⌵ DNS

DNS

1-48 DNS

DNS < > “ ”

1.3.6.2

“ ” “ WEB ”





< > “ ” “ ”



admin

“ ”

1.3.6.4

“ ” “ ”



1-52

IP SYSLOG



1-53

“ ”

1.3.6.5

“ ping ” “ tracert ” “ ”

↘ Ping

Ping

1-54 ping

IP

<

>

 **tracert**

tracert

1-55 tracert

ping

IP

<

>