

WEB

RG-S6000E

S6000E_RGOS11.4(1)B2

V .0

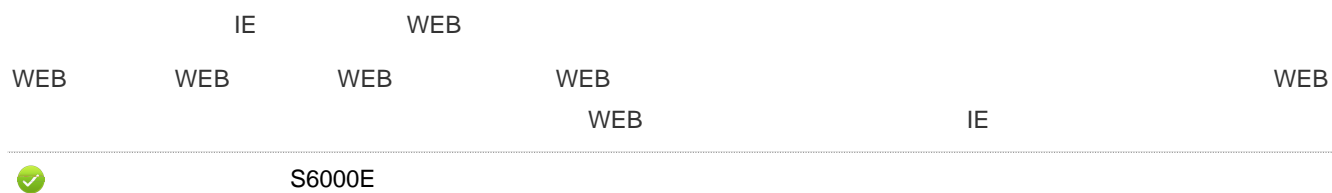
copyright © 2016





1 Eweb

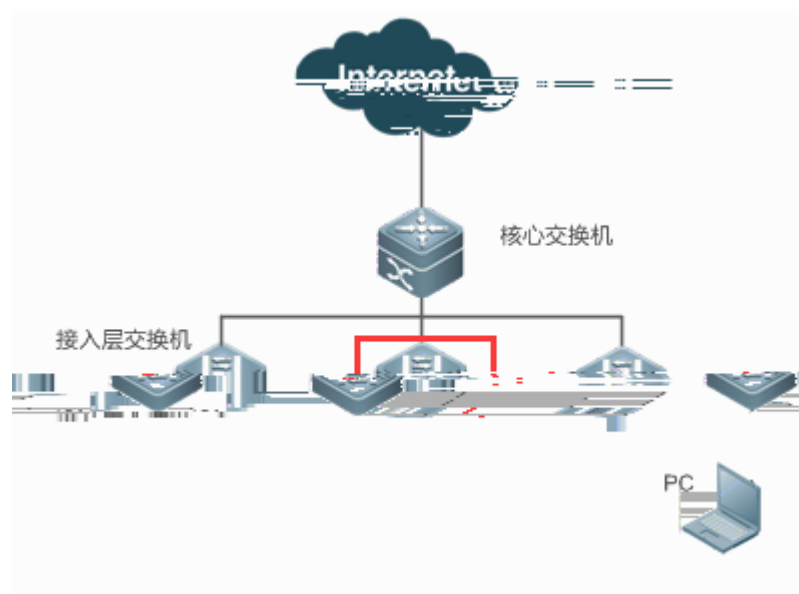
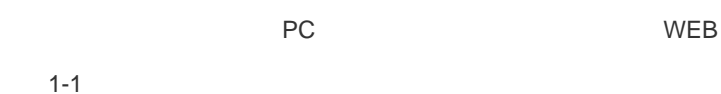
1.1



1.2

<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

	ping tracet

1.3.1

1-4

☰ 向导
✕

管理口： Gi1/0/1

IP地址： *

子网掩码： *

默认路由：

DNS服务器：

VLAN ID IP

DNS

"

"

1.3.2

" "

VLAN

1.3.2.1

1-5

首页

9

系统时间
当前时间: 2015-07-02 15:55:32
设备运行时间: 0天03时53分

设备型号:
版本信息:
设备MAC: 1414.4b77.9977

系统告警:
目前有1条系统告警信息 详细

端口信息 刷新列表

请选择插卡:

端口	输入速率	输出速率	状态	接收/发送字节	不完整/过大数据包	CRC/FCS错误包	冲突次数	
0	Gi1/0/1	0.1K	OK	连接	2688942/142438	0/0	0/0	
K	连接	3362284207/1114284	0/0	0/0	0	Gi1/0/2	0.4K	0.1
K	连接	128768/4374087446	0/0	0/0	0	Gi1/0/3	0K	0.5
<	未连接	0/0	0/0	0/0	0	Gi1/0/4	0K	0K
<	未连接	0/0	0/0	0/0	0	Gi1/0/5	0K	0K
<	未连接	0/0	0/0	0/0	0	Gi1/0/6	0K	0K
<	未连接	0/0	0/0	0/0	0	Gi1/0/7	0K	0K
未连接	0/0	0/0	0/0	0	Gi1/0/8	0K	0K	
0/10	OK	OK	未连接	0/0	0/0	0/0	0	Gi1/

1.3.2.2 VLAN

VLAN " VLAN " " Trunk "

↘ VLAN

VLAN

1-6 VLAN



1-8

端口名称	端口描述	端口速率	端口模式	端口类型	端口连接	端口IP地址	操作
Gi1/0/1	开启	自协商	自协商	连接-大网	IPV4地址：192.168.18.3.120,子网掩码：255.255.255.240	编辑	
Gi1/0/2	开启	自协商	自协商			编辑	
Gi1/0/3	开启	自协商	自协商			编辑	
Gi1/0/4	开启	自协商	自协商	pc-邢台学院		编辑	
Gi1/0/5	开启	自协商	自协商	pc-山东畜牧兽医职业技术学院		编辑	
Gi1/0/6	开启	自协商	自协商	pc-河南财经大学		编辑	
Gi1/0/7	开启	100M	自协商	pc-云南财经大学		编辑	
	编辑	Gi1/0/8	开启	自协商	自协商		
	编辑	Gi1/0/9	开启	自协商	自协商		
	编辑	Gi1/0/10	开启	自协商	自协商		

显示 10 条 共 107 条





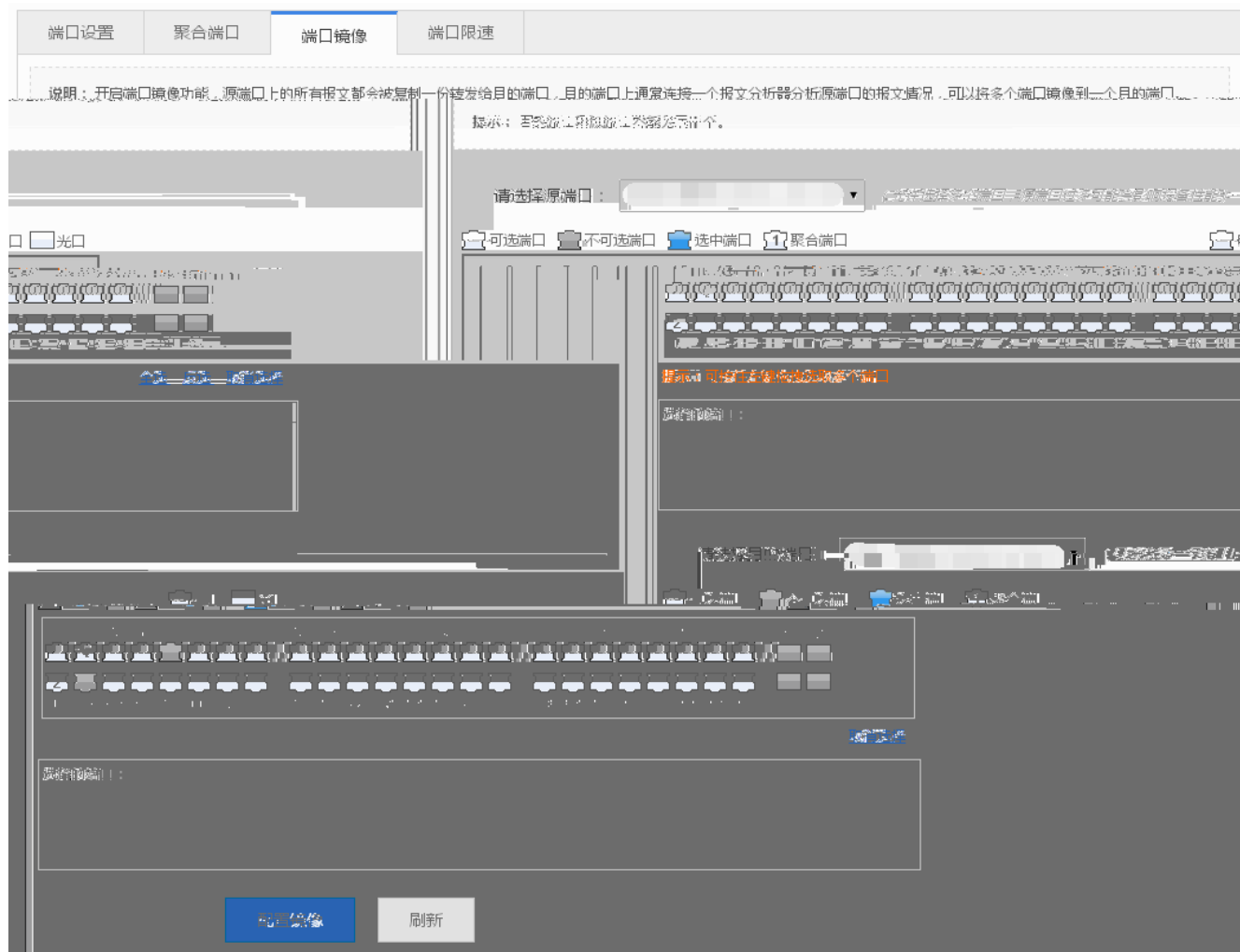
ARP

ARP

MAC VLAN



1-10



web



1-11

端口设置 聚合端口 端口镜像 端口限速

+ 批量配置限速端口 × 批量删除限速端口

操作	<input type="checkbox"/>	端口	输入速率(Kbps)	输出速率(Kbps)
编辑 删除	<input type="checkbox"/>	Gi0/9	102400	102400

显示 10 条 共 10 条

首页 < 上一页 1 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

<input type="checkbox"/>	MAC地址	VLAN ID	操作
<input type="checkbox"/>	0002.0002.0003	4	编辑 删除

显示: 条 共1条

⏪ 首页
◀ 上一页
1
下一页 ▶
末页 ⏩

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的优先级高。

[+ 添加静态路由](#) [+ 添加默认路由](#) [X 删除选中路由](#)

<input type="checkbox"/>	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

生成树全局设置 生成树端口设置 RLDP设置

全局设置

生成树开关： ON

优先级： 范围(0-15)，默认8 握手时间： 范围(1-10)秒，默认2

老化时间： 范围(0-10)秒，默认300 转发延迟： 范围(1-30)秒，默认15

生成树模式：

保存设置

MST 设置

[+ 添加实例](#) [X 删除选中实例](#)

N	优先级	操作	<input type="checkbox"/>	实例值	VLAN
	8	默认实例，不可编辑	<input type="checkbox"/>	0	ALL

1-17

" MSTP"

MST

VLAN

"

"

"

"

" "

< >

< > "

"

1

" "

"

"

2

" "

< >

"

"

"

"

0



1-17

2 " RLDLP " < > " " "

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的作用便是窥探那个端口需要组播流，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 X 删除选中组策略 IGMP Snooping开关：

策略图标	策略地址	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

≡ 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



外置web认证	高级设置
最大HTTP会话数： <input type="text" value="255"/> (范围1-255，默认255) 防止同一个未认证用户发起过多的HTTP连接请求，需要限制未认证用户的最大HTTP会话数。	
默认3) 设置维持重定向连接的超时时间，防止未认证用户不发GET/HEAD报文，而又长时间占用TCP连接。	
重定向超时时间： <input type="text" value="3"/> (范围1-10秒)	
在线信息更新时间： <input type="text" value="100"/> (范围00-0000)	
重定向HTTP端口： <input type="text" value="80"/>	

1.3.4

" "

DHCP Snooping

ARP

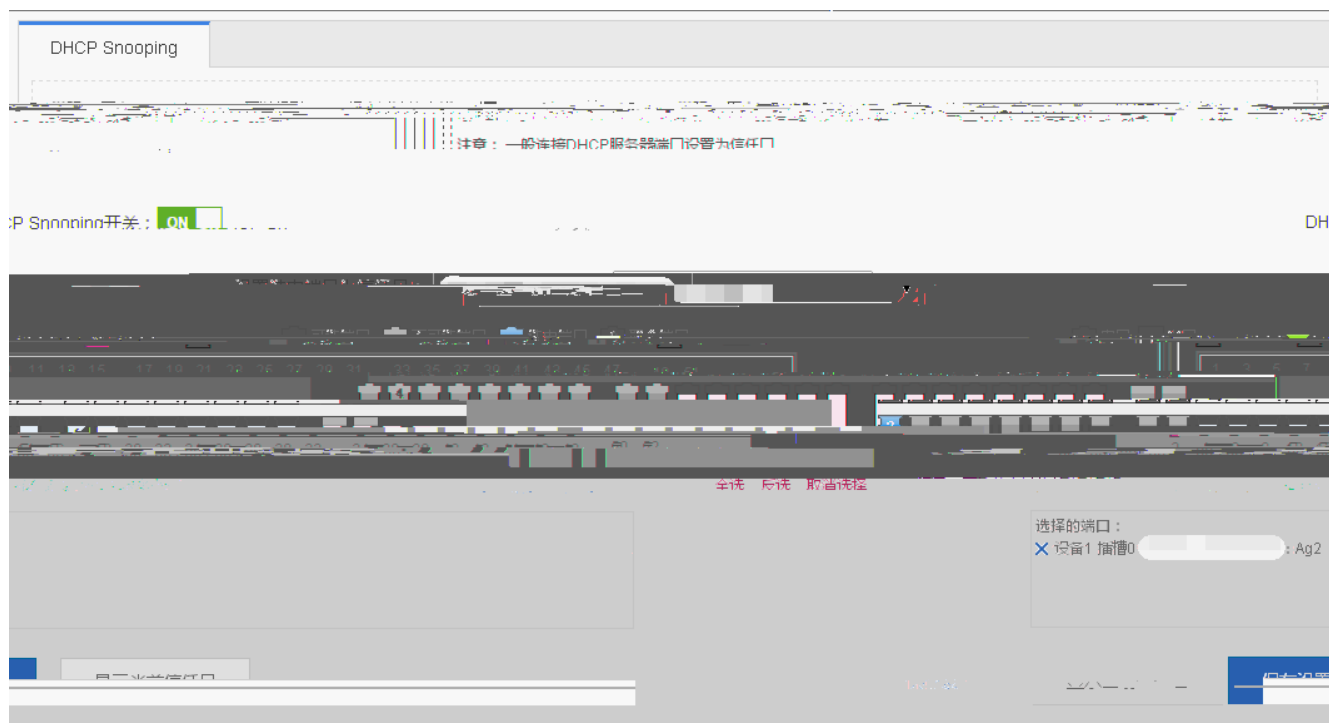
IP Source Guard

NFPP

1.3.4.1 DHCP Snooping

DHCP Snooping

1-22 DHCP Snooping



DHCP SERVER
DHCP

DHCP

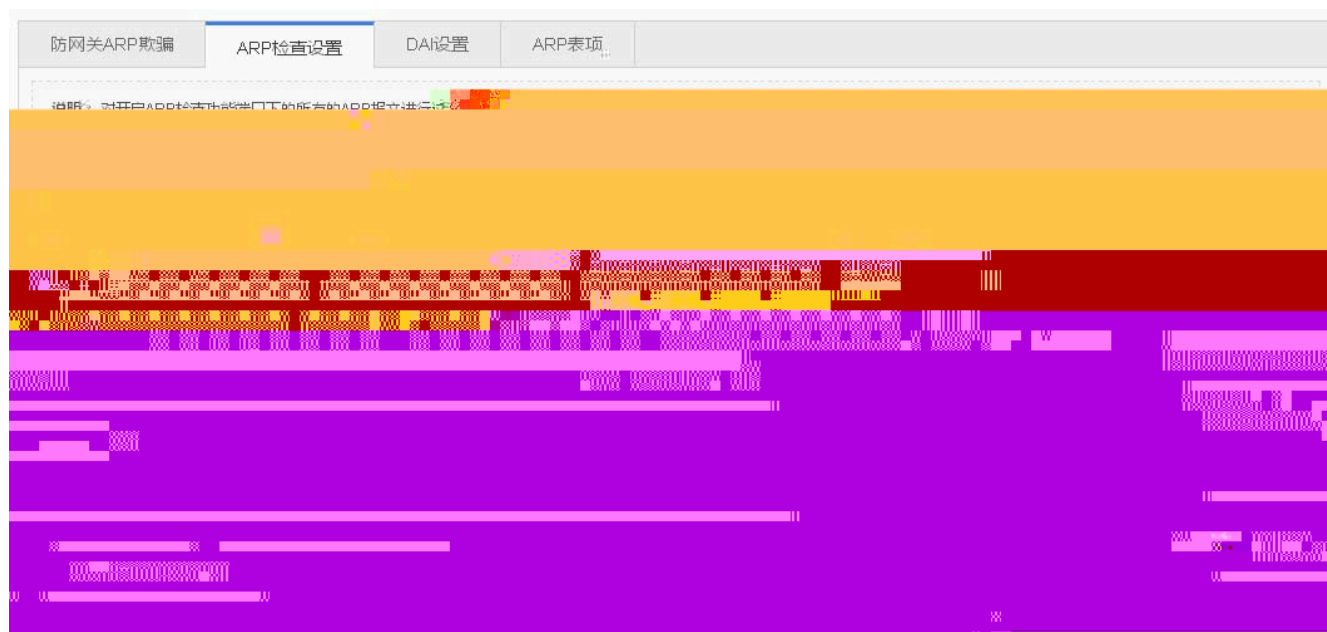
DHCP SERVER
< >

1.3.4.2 ARP



" ARP " ARP ARP DAI ARP

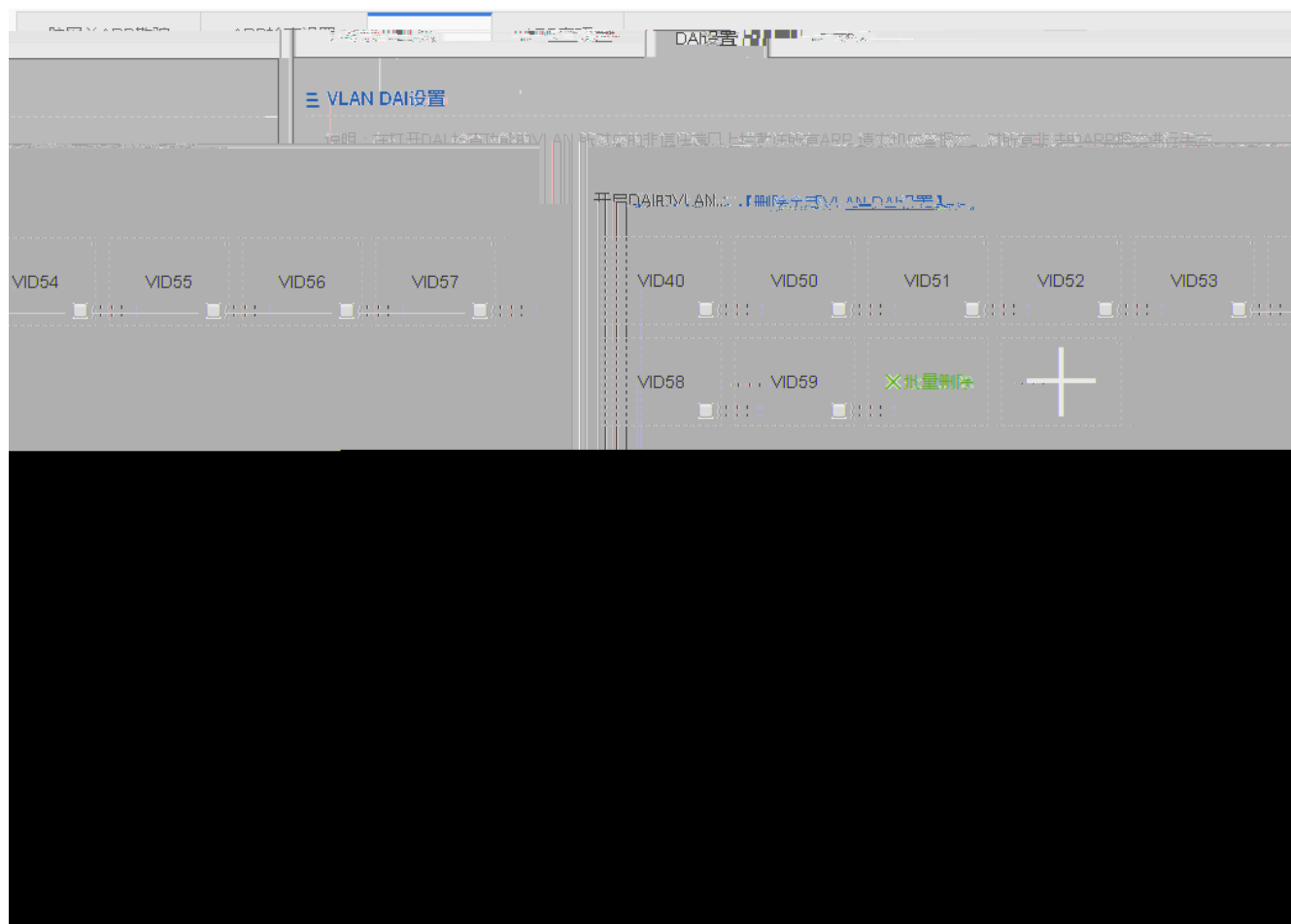
↓ ARP

1-23 ARP



ARP

-  ARP
- < ARP > ARP
-  DHCP Snooping ARP
- DAI
- 1-25 DAI



1 VLAN DAI

DAI VLAN

2 DAI

DAI



DAI



DAI



DAI



DHCP Snooping

ARP



ARP

1-26 ARP



- 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

X 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					

[前一页](#)
[末页](#)

 显示 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

<input type="checkbox"/>	端口	IP地址	MAC地址	VLAN ID	操作
无记录信息					

显示 10 条共0条

● 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】](#)

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】](#)

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

1.3.4.6

1-32

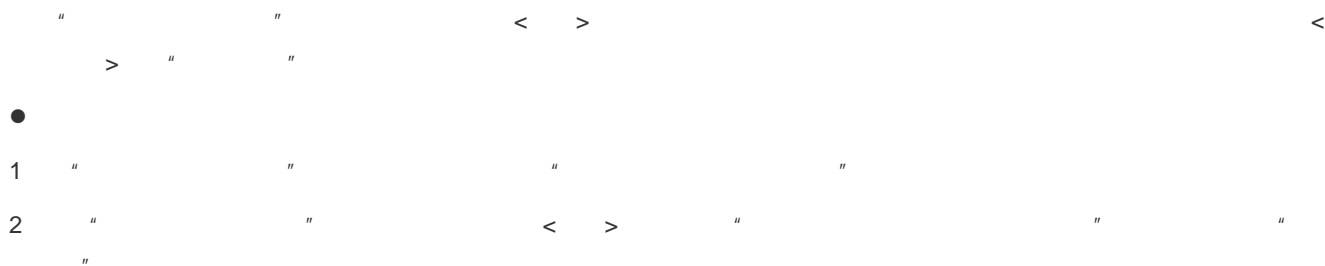
风暴控制

+ 添加风暴控制端口 X 删除选中的风暴控制端口

<input type="checkbox"/>	端口	广播	组播	单播	操作
<input type="checkbox"/>	Gi0/16	90%	-	-	<input type="button" value="编辑"/> <input type="button" value="删除"/>

显示 条共1条

◀ 首页 ◀ 上一页 1 下一页 ▶ ▶ 末页



1.3.5

1.3.5.1

1-33



1.3.5.2 DHCP

" DHCP " DHCP

ES224GT

↘ DHCP

DHCP

1-34 DHCP

-

	IP	MAC	"	"	"	"
●			<	>		< >
	"	"				
●						
1	"	"	"	"		
2	"	"	<	>	"	" " "

↓

1-36

DHCP配置
静态地址分配
客户端列表

把MAC地址绑定到动态获取的IP上
删除选中客户端
基于IP地址查询

<input type="checkbox"/>	已分配的IP地址	MAC地址	地址租期	IP分配方式	操作
无记录信息					

显示: 10 条 共0条

 << 首页 < 上一页 下一页 > 末页 >>

确定

- IP

IP
IP

- MAC

MAC	IP
"	"
"	MAC
"	IP

1.3.5.3 ACL

ACL

ACL

1-37ACL

ACL列表

test 添加ACL 删除ACL + 添加ACE规则 X 删除选中 ACL列表

序号	源IP/通配符	源端口	访问控制	协议	目的IP/通配符	目的端口	生效时间	状态	操作
无记录信息									

1 10 条共 10 条

- ACL
- " ACL" ACL " " " " " ACL
- ACL
- ACL ACL " ACL" " "
- ACL
- ACL IP " " " " " ACL
- ACL
- " ACL " < > ACL <
- ACL
- 1 " ACL " " "
- 2 " ACL " < > " " " "

● ACL

ACL " " " " ACL

● ACL

" ACL " < > ACL <
> " "

● ACL

" ACL " " "

▾ ACL

ACL

1-39 ACL

操作	ACL	应用端口	过滤方向
<input type="checkbox"/>	test	Gi0/24	in

应用端口 X 删除ACL应用端口 + 添加ACL

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

	"	"	<	>	"	"	"	"
●						"	"	"
●	"	"	<	>			<	>
	"	"						
●								
1	"	"	"	"				
2	"	"	<	>	"	"	"	"

↓

1-42

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](#) [X 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

●					"	"	"	"
●								
1	"	"	<	>				
2	"	"	<	>	"	"	"	"

1.3.6

" "

1.3.6.1

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

↓ 1--

1-43



•

" Internet "

< > " "



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

telnet



1-45

- /
-
- < >
- ↓

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: * (范围80,1025-65535)

登录超时:

设备位置:

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 " " tracet " " "

↳ Ping

Ping

1-54 ping

IP

<

>

↘ **tracert**

tracert

1-55 tracert

ping

IP

<

>