



WEB

RG-S6000E

S6000E_RG OS11.4(1)B2

V2.0

copyright © 2016



-
-
-

-

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

-

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

-

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

- 7×24

4008-111-000

-

<http://bbs.ruijie.com.cn/portal.php>

-

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

-

4008111000@ruijie.com.cn

1.

[] []

{ x | y | ... }

[x | y | ...]

//

2.





1 Eweb

1.1



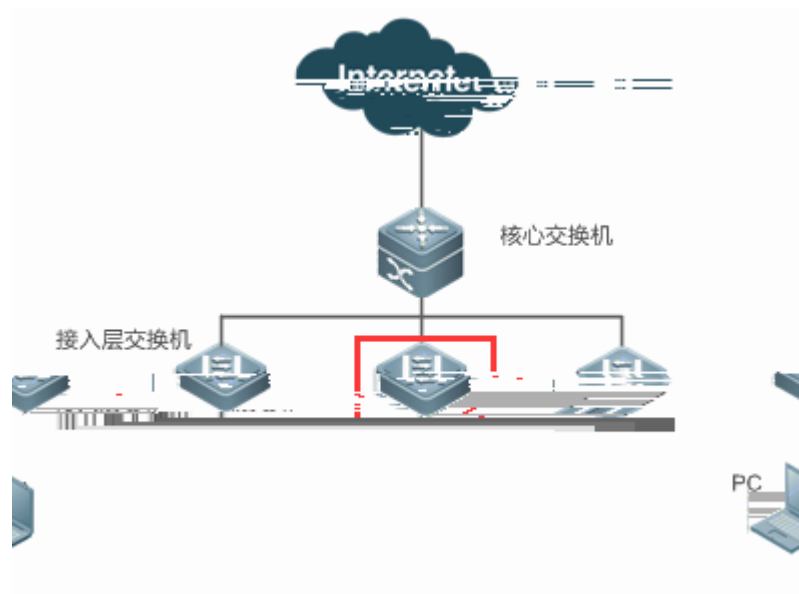
1.2

<u>WEB</u>	WEB
------------	-----

1.2.1 WEB

PC WEB

1-1



PC ping



RG交换机



极简网络，新一代交换机

登录

[忘记密码?](#)

[English ▶](#)



保存设置	
+	
×	
全选 反选 取消选择	
*	
	
	



可选端口
 不可选端口
 选中端口
 聚合端口

电口
 光口

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51	53	55	57	59	61	63	65	67	69	71	73	75	77	79	81	83	85	87	89	91	93	95	97	99

全选
反选
取消选择
提示：可按住左键拖拽选取多个端口

端口：5/99

选择的端口：





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

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

1.3.2.2 VLAN

VLAN " VLAN " " Trunk "

VLAN

VLAN

1-6 VLAN



1-8

+ 批量设置端口						
端口名称	端口描述	端口速率	端口模式	端口类型	端口连接	端口速率
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-河南财经大学		编辑
开启	自协商	自协商				Gi1/0/8
开启	自协商	自协商				Gi1/0/9
开启	自协商	自协商				Gi1/0/10

共107条

1 / 10 页





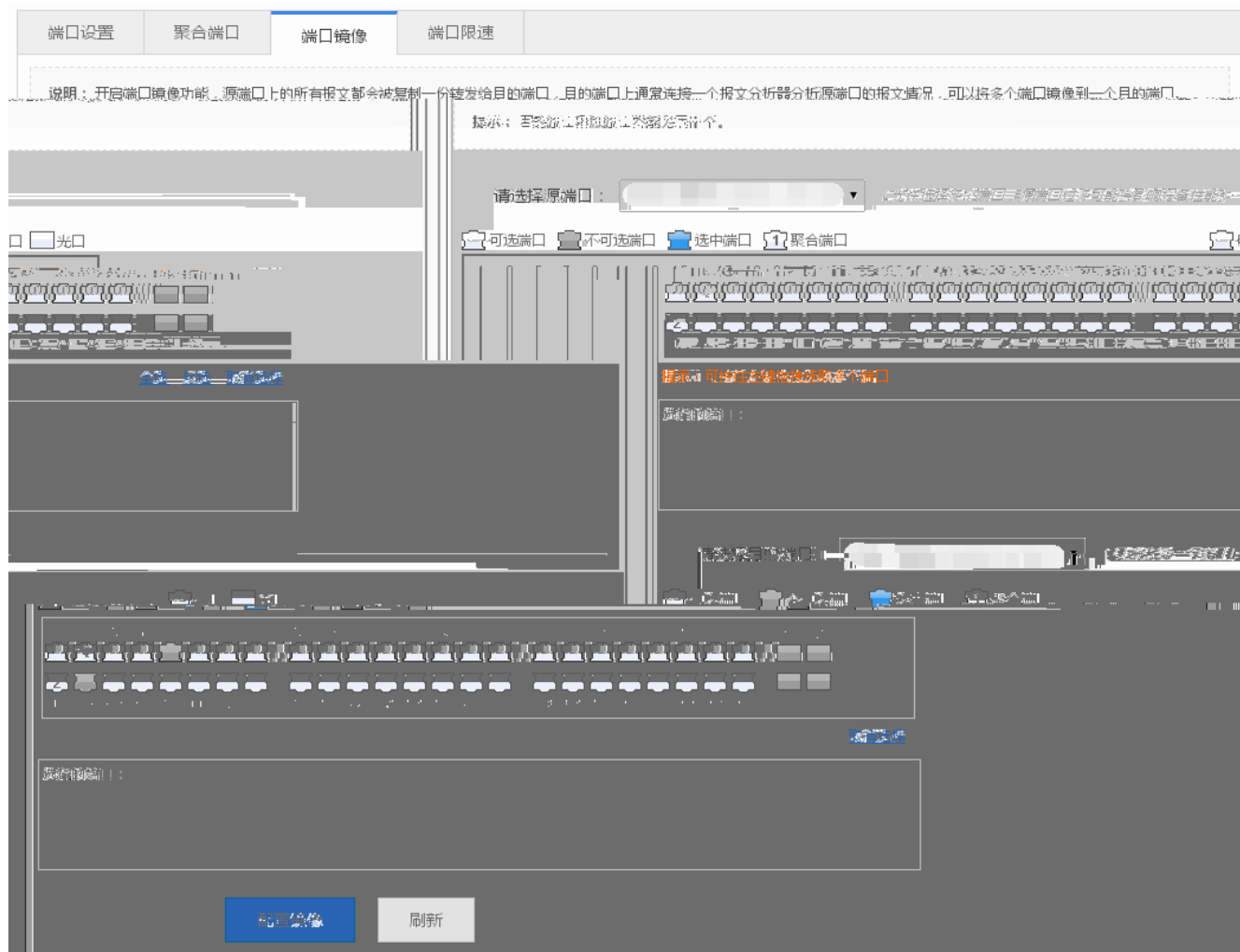
ARP

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: 10 ▼ 条 共1条

◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶▶ 1 [确定](#)

MAC

VLAN ID

"

"

"

"

"

"

<

>

<

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 条 共0条

[首页](#)
[< 上一页](#)
[下一页 >](#)
[末页](#)

[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

RLDAP设置

三 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(10-300)秒，默认(30)

转发延迟： 范围(1-30)秒，默认(15)

生成树模式：

保存设置

三 MST 设置

+ 添加实例 -X 删除选中实例

VLAN	优先级	操作
ALL	8	默认实例，不可编辑

<input type="checkbox"/>	实例值
<input type="checkbox"/>	0

" 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： 范围(2-15s)

探测次数： 范围(2-10)

恢复周期： 范围(30-86400s)

[保存设置](#)

端口RLDP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。

检测类型	故障处理	操作	端口
无记录信息			

[首页](#) | [上一页](#) | [下一页](#) | [末页](#) | [确定](#) | 显示 10 条共 0 条

1 RLDP

RLDP RLDP RLDP < > "

2 RLDP

● RLDP
" " " " " " " " RLDP
" RLDP "

● RLDP
" RLDP " < > RLDP
< > " "

●
" RLDP " " RLDP "

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)
默认100) 设置在线信息更新的超时时间。	在线信息更新时间： <input type="text" value="100"/> (范围00-9999)
最多配置10个。	重定向HTTP端口： <input type="text" value="80"/> (端口号范围1-65535) 多个用“ ”隔开，最

1.3.4

" "

DHCP Snooping

ARP

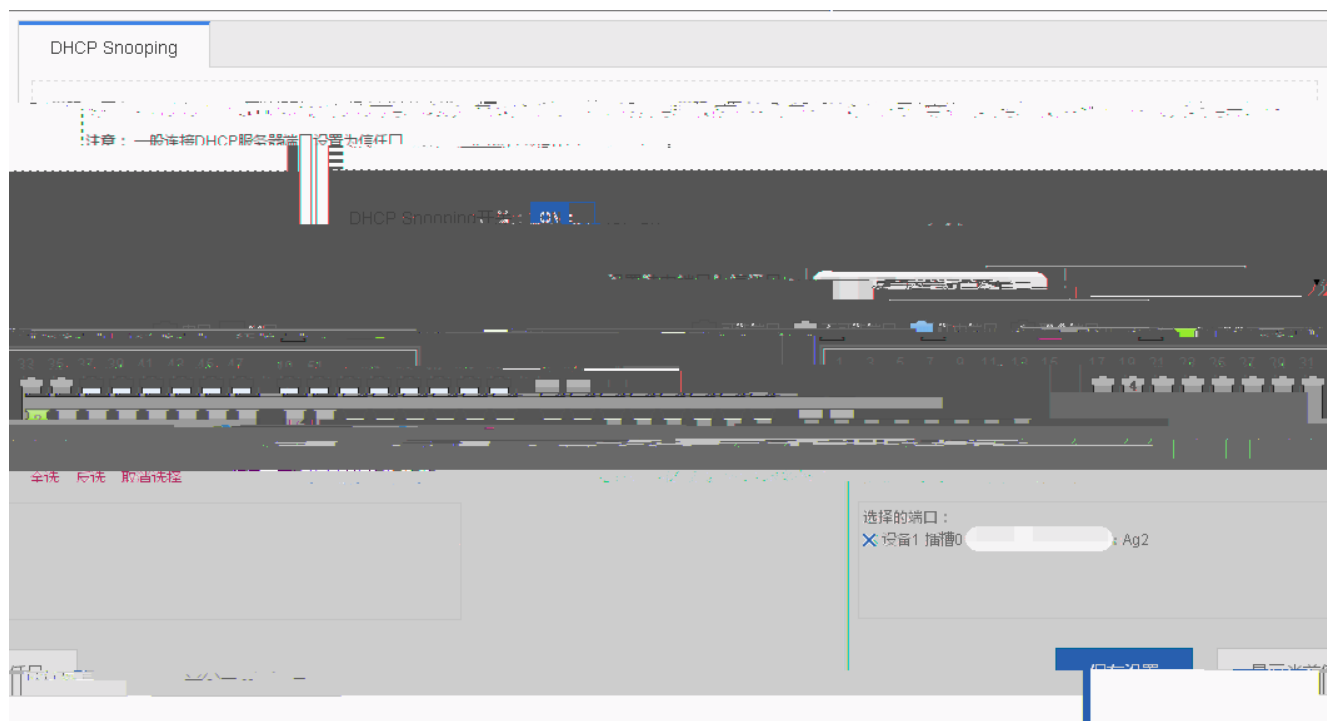
IP Source Guard

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

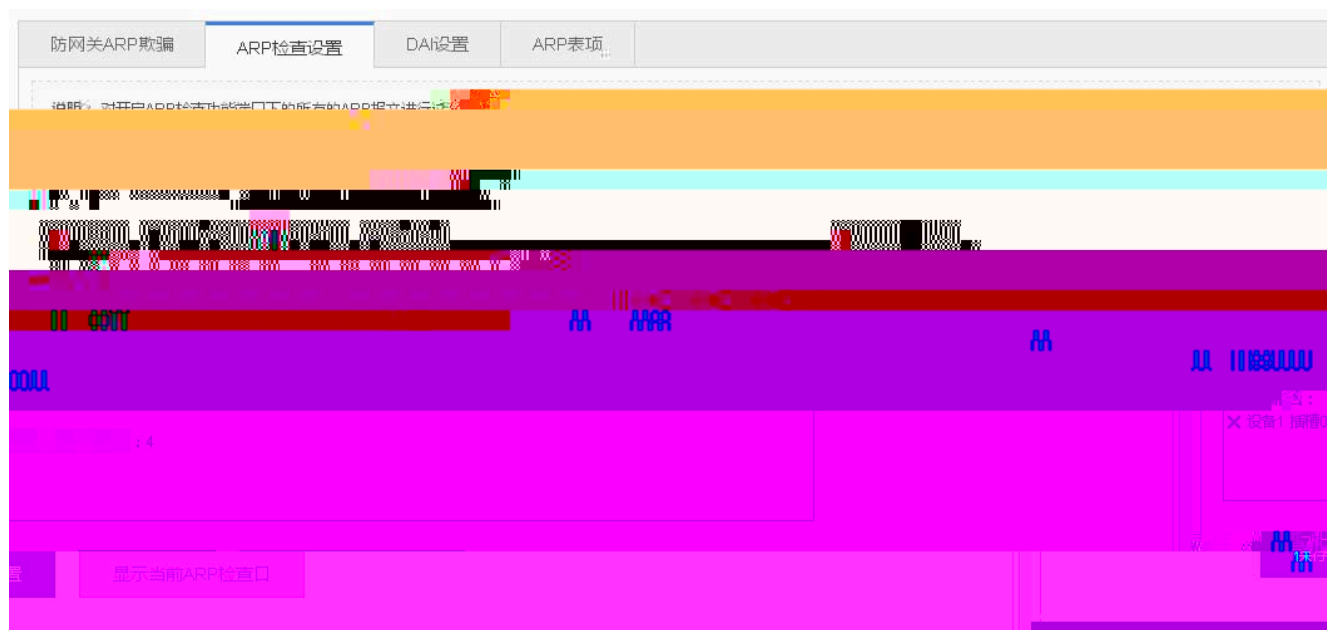
ARP

DAI

ARP

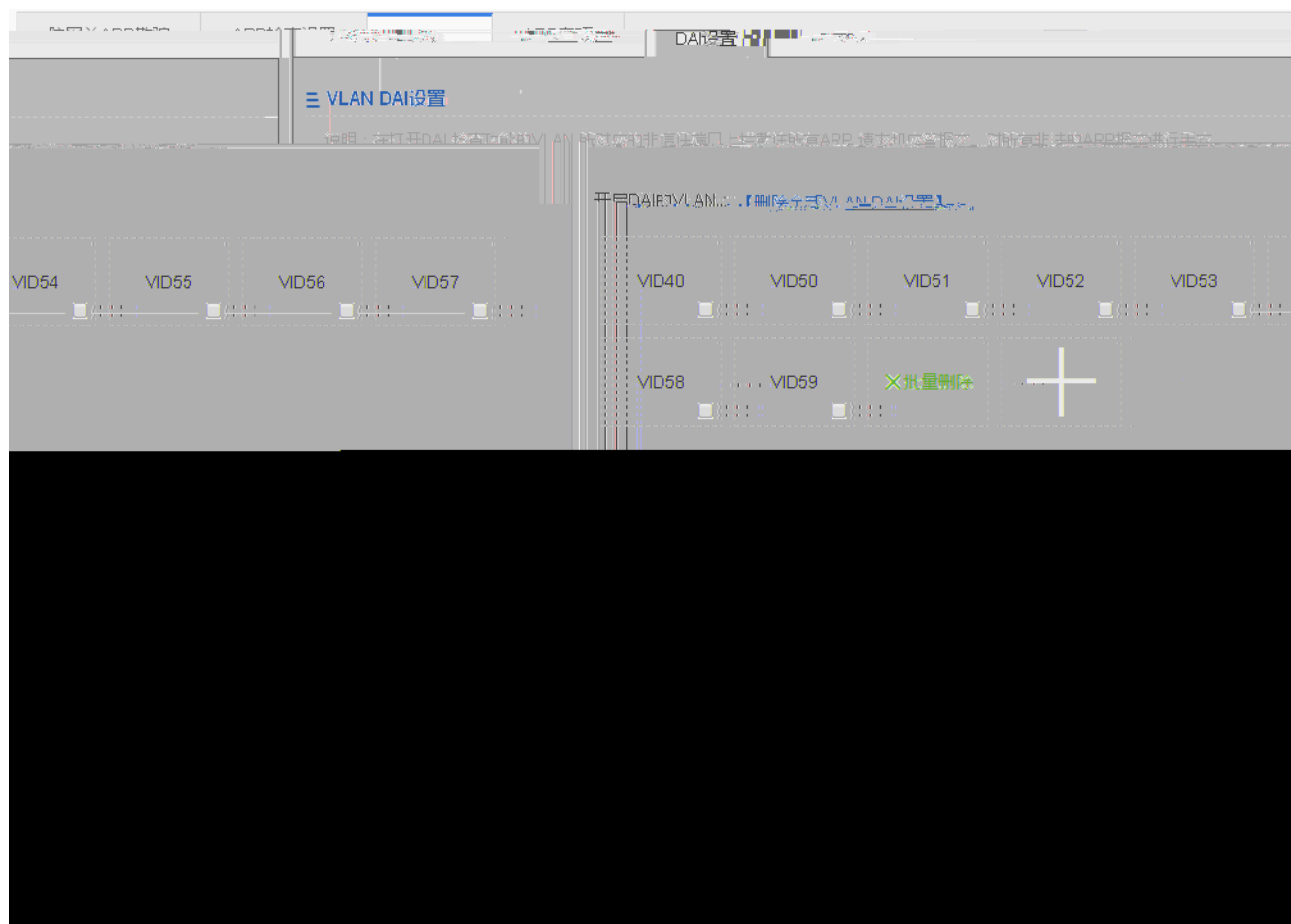
↓ ARP

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 × 删除选中的安全口

	端	限定MAC数	老化时间	违例处理方式	操作
无记录信息					

页 < 上一页 下一页 > 末页 >>
1 确定
显示: 10 条 共0条
<< 首页

-

	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 X 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

首页 上一页 下一页 末页

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

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竭！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: 10 条共1条

« 首页 < 上一页 1 下一页 > 末页 »

" " < > <

> " "

●

1 " " " "

2 " " < > " " "

"

1.3.5

1.3.5.1

1-33



•

IP MAC " " " "

•

" " < > < >

" " " "

•

11 ħ U DUA•zÍ" z z ! k_

ACL列表 ACL时间 应用ACL

添加ACL 删除ACL + 添加ACE规则 X 删除选中

ACL列表: test

序号	源IP/通配符	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

- 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

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 X 删除选中的分类

<input type="checkbox"/>	分类名	ACL	操作
<input type="checkbox"/>	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。

策略列表: dsaff [添加策略](#) [删除策略](#) + 添加策略规则 X 删除选中规则

带宽超出处理	操作	<input type="checkbox"/>	类名	带宽(Kbps)	突发流量(KBytes)

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

-
-

	"	"	<	>	"	"	"	"
●					"	"	"	"
●	"	"	<	>			<	>
	"	"						
●								
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 × 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:

WEB

< > " "

↳ **SNMP**

SNMP

1-47 SNMP

:(03

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

<

>