



WZB

RG-S6000E

S6000E\_RG OS11.4(1)B12

V2.0

copyright © 201



- 
- 
- 

- 

<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](mailto:4008111000@ruijie.com.cn)

1.

[ ] [ ]

{ x | y | ... }

[ x | y | ... ]

//

2.



# 1 Eweb

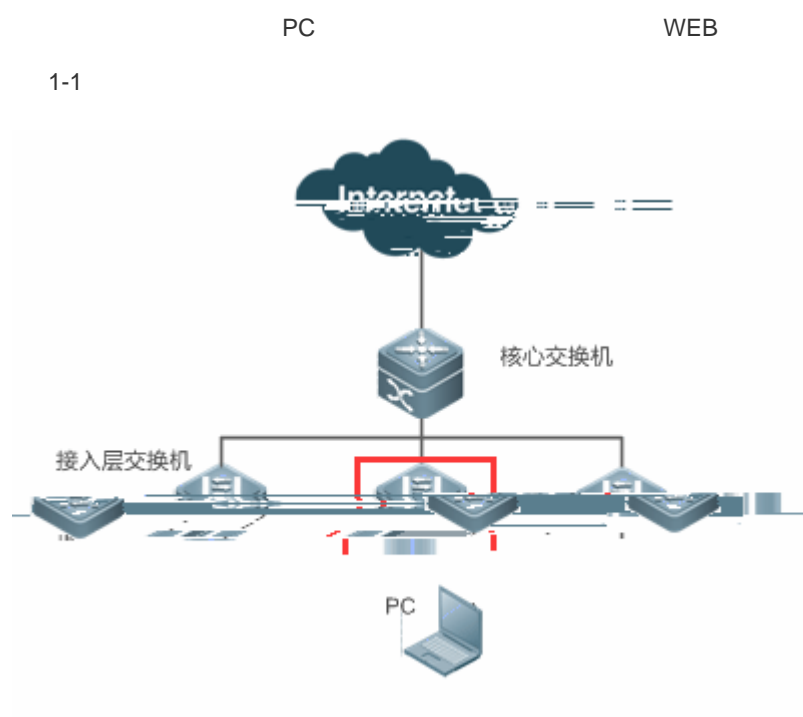
## 1.1



## 1.2

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

### 1.2.1 WEB







# RG交换机

极简网络，新一代交换机

登录

[忘记密码?](#)

[English ▶](#)



<b>保存设置</b>	
+	
X	
全选 反选 取消选择	
*	



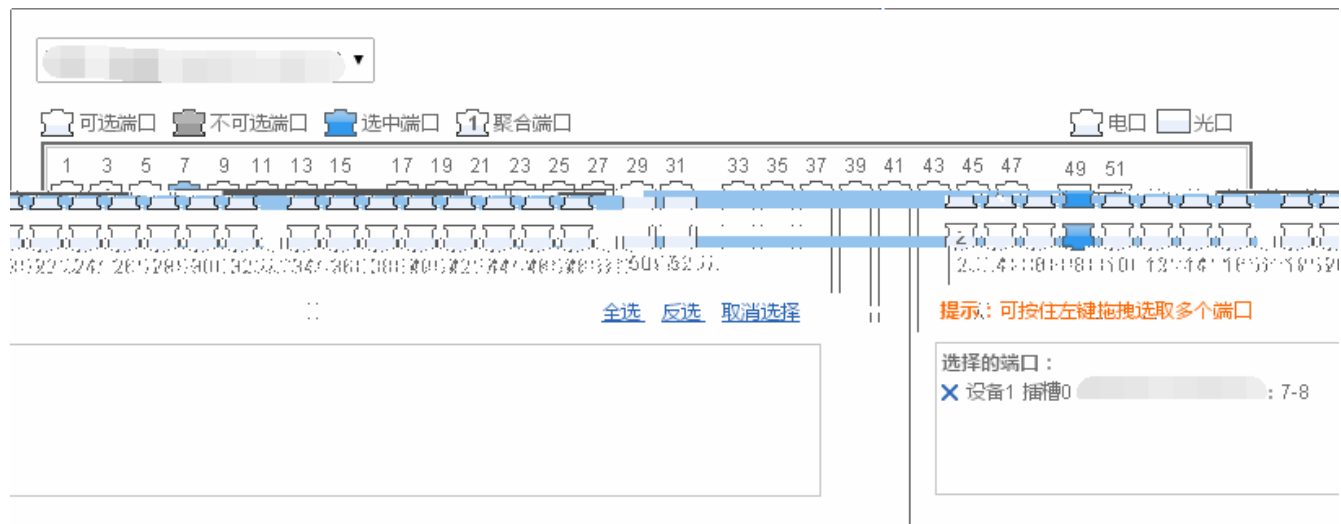
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

可选端口 不可选端口 选中端口 聚合端口 电口 光口

按住左键拖拽选取多个端口 全选 反选 取消选择 提示：可

Port: 5000





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: 2015-07-02 15:55:32 设备型号: 版本信息: 设备运行时间: 0天03时53分 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:

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	端口	输入速率	输出速率	
OK	连接	2688942/142438	0/0	0/0	0	Gi1/0/1	0.1K	
0	Gi1/0/2	0.4K	0.1K	连接	3362284207/1114284	0/0	0/0	
0	Gi1/0/3	0K	0.5K	连接	128768/4374087446	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	未连接	0/0	0/0	0	
0	0/0	0/0	0/0	0	Gi1/0/10	0K	0K	未连接

## 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	<a href="#">编辑</a>	
Gi1/0/2	开启	自协商	自协商			<a href="#">编辑</a>	
Gi1/0/3	开启	自协商	自协商			<a href="#">编辑</a>	
Gi1/0/4	开启	自协商	自协商	pc-邢台学院		<a href="#">编辑</a>	
Gi1/0/5	开启	自协商	自协商	pc-山东畜牧兽医职业技术学院		<a href="#">编辑</a>	
Gi1/0/6	开启	自协商	自协商	pc-河南财经大学		<a href="#">编辑</a>	
Gi1/0/7	开启	100M	自协商	pc-河南财经大学		<a href="#">编辑</a>	
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







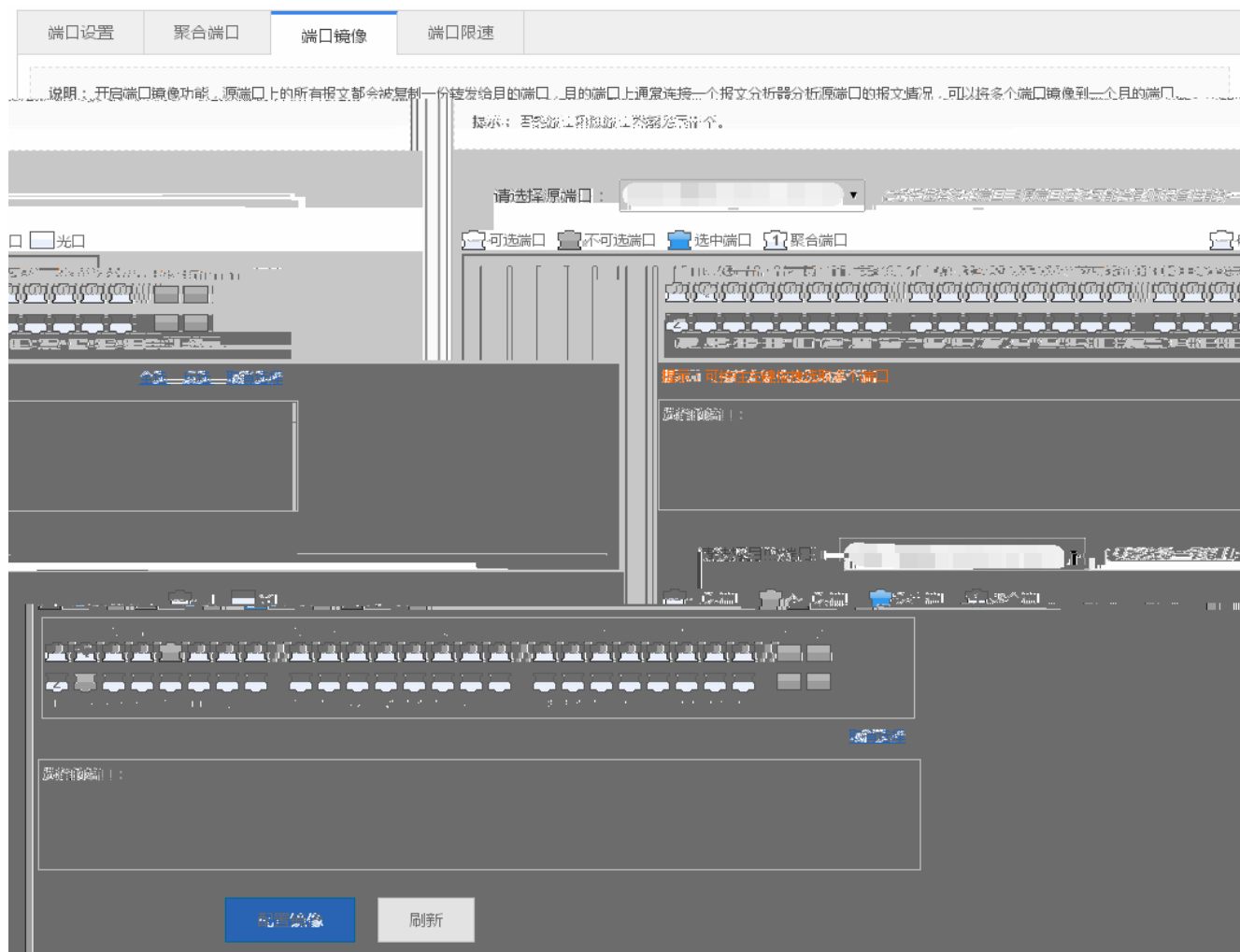
ARP

ARP

MAC VLAN



1-10



web







1-14

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	<span style="background-color: #0070c0; color: white; padding: 2px 5px;">编辑</span> <span style="background-color: #ccc; padding: 2px 5px; margin-left: 5px;">删除</span>

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 " " &lt; &gt; " " " "

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(0-30)秒, 默认20

转发延迟:  范围(0-30)秒, 默认15

生成树模式

MSTP

保存设置

MST设置

+ 添加实例 X 删除选中实例

VLAN	优先级	操作	实例值
ALL	8	默认实例, 不可编辑	0

" 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： ON

策略名称	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

● " " " "

● " " " " " "

● " " " " " "

1 " " " "

2 " " " " " "

### 1.3.3.5 DHCP

DHCP

1-19 DHCP

## 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400) 设置在未登录信息的时间间隔内, 每隔多少秒刷新一次	
在线信息更新时间： <input type="text" value="400"/> (范围30-600秒)	
(编号号范围1-65535) 多个用户"顺序"最多可配置10个。	
重定向HTTP端口： <input type="text" value="80"/>	

## 1.3.4

" "

DHCP Snooping

ARP

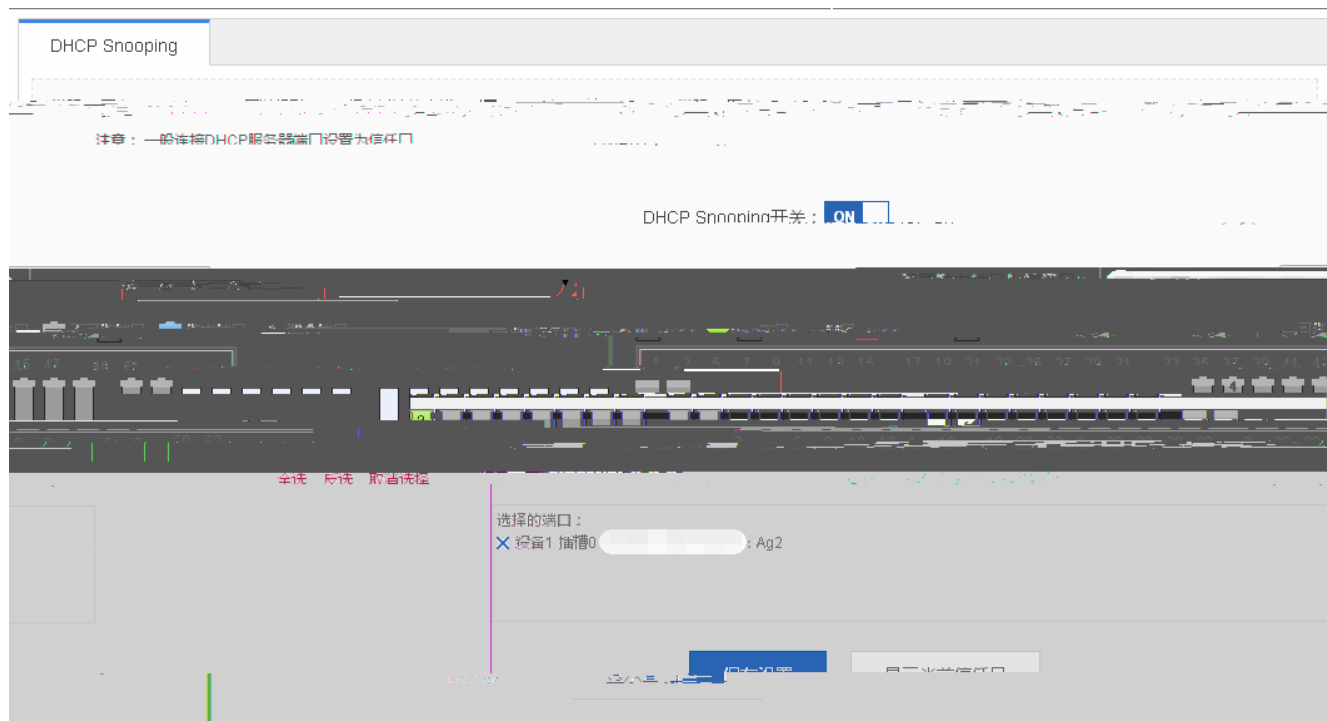
IP Source Guard

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

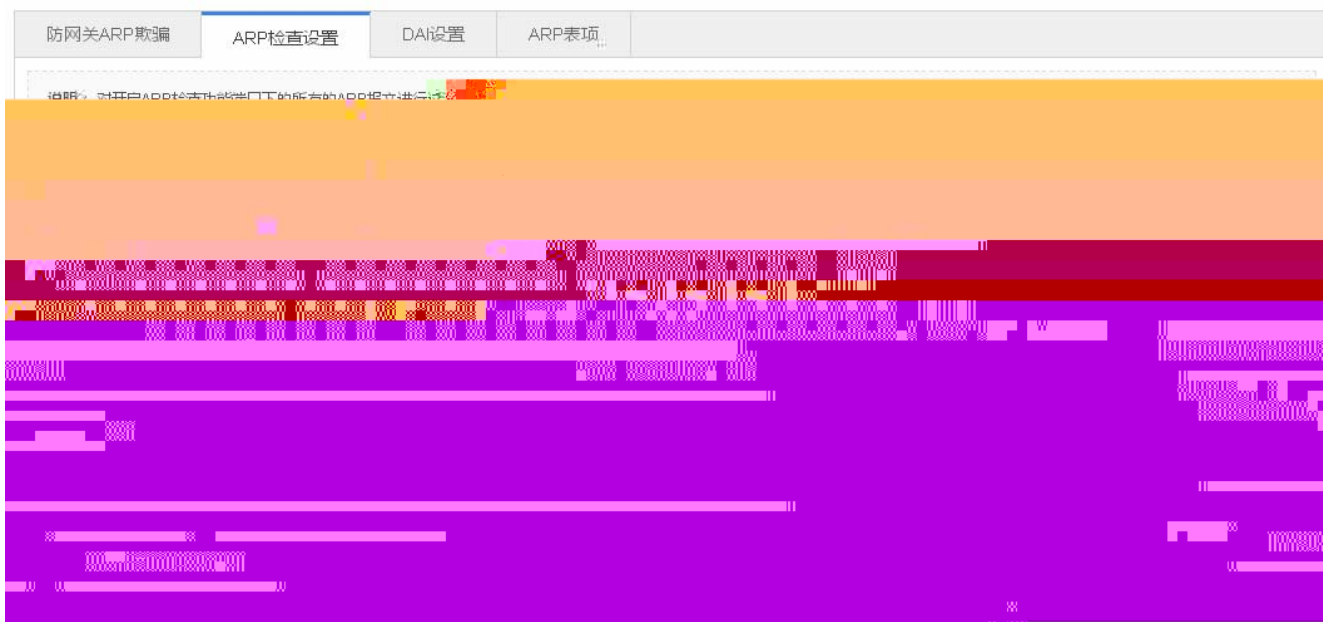
DAI

ARP

↓ ARP

1-23 ARP





ARP



ARP



ARP



ARP



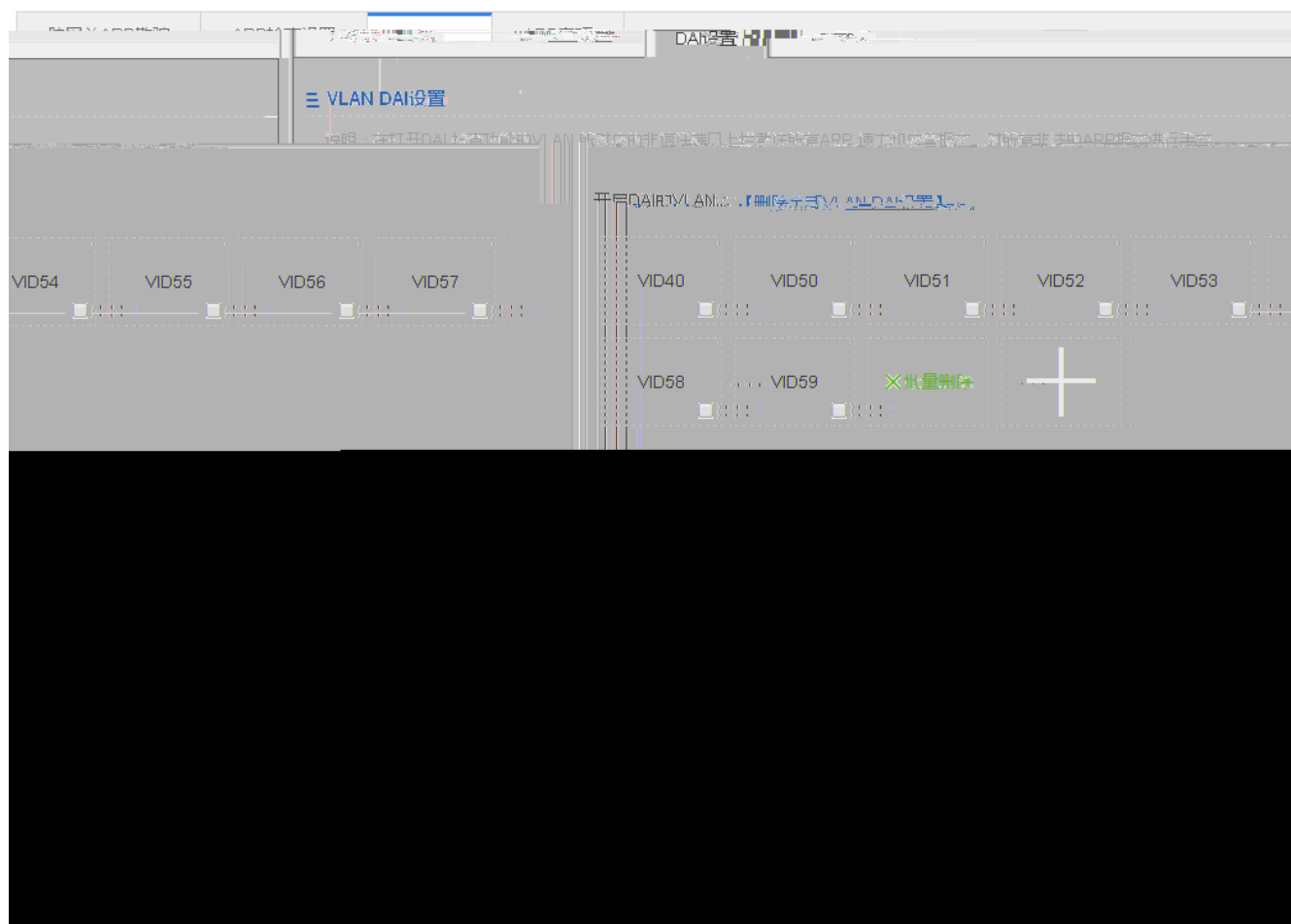
DHCP Snooping

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    × 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

<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 " " < > " "

" "

### 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，防止非法IP扫描攻击设备。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池被恶意请求使地址池耗尽，导致合法用户获取不到IPv4无法上网。  
[【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**。  
[【ND防攻击列表】](#)

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 × 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 ▶



DHCP

1-34 DHCP

DHCP配置		静态地址分配	客户端列表
--------	--	--------	-------

名称	地址范围	默认网关	租用时间	DNS	操作
xlsp40	40.40.0.1-40.40.255.254	40.40.255.254	20小时		<a href="#">编辑</a> <a href="#">删除</a>

[首页](#)
[上一页](#)
1
[下一页](#)
[末页](#)

显示 10 条 共1条

- DHCP
    - IP " " " " DHCP
  - DHCP
    - " DHCP " < > DHCP < >
    - " "
  - DHCP
    - 1 " DHCP " " DHCP"
    - 2 " DHCP " < > " DHCP " " "
  - DHCP
    - <DHCP > DHCP
- ↓

1-35

DHCP配置		静态地址分配	客户端列表
--------	--	--------	-------

[+ 添加静态地址](#)
[X 删除选中地址](#)

<input type="checkbox"/>	客户名称	客户端IP	掩码	网关	客户端MAC	DNS服务器	操作
无记录信息							

[首页](#)
[上一页](#)
1
[下一页](#)
[末页](#)

10 条 共0条

- 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 >> 1 确定

- IP
- IP
- 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

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

- ACL
- " ACL" ACL " " " " " ACL
- ACL
- ACL
- 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	<a href="#">编辑</a> <a href="#">删除</a>

显示: 10 条 共1条      << 首页 < 上一页 1 下一页 > 末页 >>    1    [确定](#)

ACL

" " " "

" " &lt; &gt; &lt; &gt; "

"

1

" " " "

2

" " &lt; &gt; " " " "



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。

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

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](#) [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

的密码)

### Telnet密码修改(修改telnet和enable

用户名：admin

新密码：

确认密码：

保存设置

- Web

Web

< >



web

enable

- Telnet

telnet



- /
- 
- < >
- ↓

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

SNMP

SNMP

Trap

< > " "

↳ **DNS**

DNS

1-48 DNS

DNS

< > " "

### 1.3.6.2

" " " WEB "



1-49



< > " " " "



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

<

>