



copyright © 2021



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

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

7\*24h

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

7\*24h

4008-111-000

--

<http://www.ruijie.com.cn/special/fw/tool/xryf/>

4008111000@ruijie.com.cn

APP

1.

<>		< >
□		

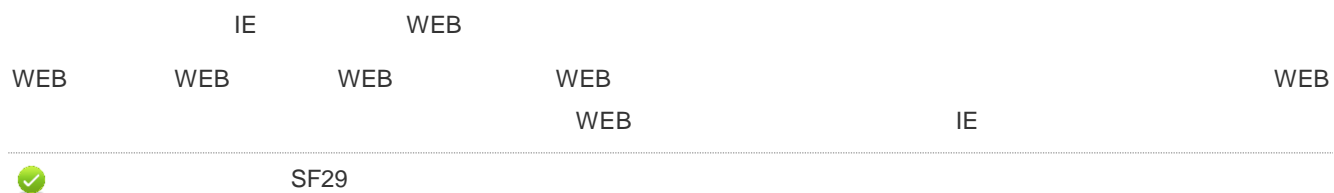


/

3.

# 1 Eweb

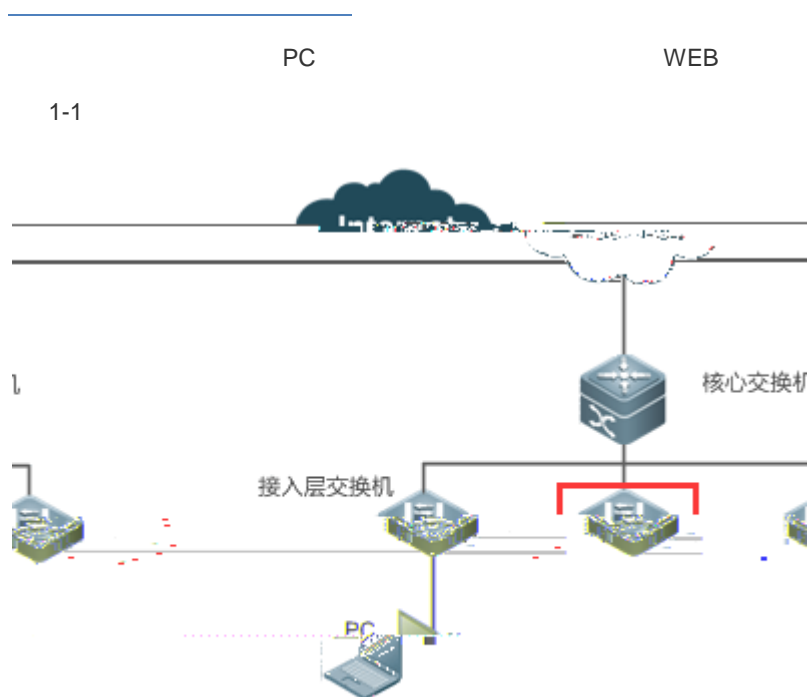
## 1.1



## 1.2



### 1.2.1 WEB



PC ping

WEB



- WEB WEB PC
- IE8~IE11 360 WEB
- 1024\*768 1280\*1024 1440\*960 1920\*1080



WEB

http://X.X.X.X IP

1-2



## RG交换机

极简网络，新一代交换机

支持的浏览器：IE8-IE11，谷歌，360浏览器

请输入管理员账户...

请输入管理员密码...

登录

[忘记密码?](#)

[English](#)

< >

/

admin / admin

## 修改密码

用户名： admin

确认密码： 请输入新密码...

修改

当前使用默认密码，为提升系统安全性，请修改密

WEB

W

Ruijie 交换机 eWEB 设备型号: [ ] 详细

向导 诺云管理 客服 更多 退出

常用 首页

VLAN管理

端口管理

端口信息 刷新列表

端口	输入速率	输出速率	状态(端口实际速率)	接收/发送字节	不完整/过大数据
Gi0/1	0.8K	0K	连接(1000M)	9584659364/43009566	0/0
Gi0/2	0K	0K	未连接	0/0	0/0
Gi0/3	0K	0K	未连接	0/0	0/0
Gi0/4	0K	0K	未连接	0/0	0/0
Gi0/5	0K	0K	未连接	0/0	0/0
Gi0/6	0K	0K	未连接	0/0	0/0
Gi0/7	0K	0K	未连接	0/0	0/0
Gi0/8	0K	0K	未连接	0/0	0/0
Gi0/9	0K	0K	未连接	0/0	0/0
Gi0/10	0K	0K	未连接	0/0	0/0

包 CRC/FCS错误包 冲突次数

显示 10 条 共28条

首页



Eweb

" Eweb "

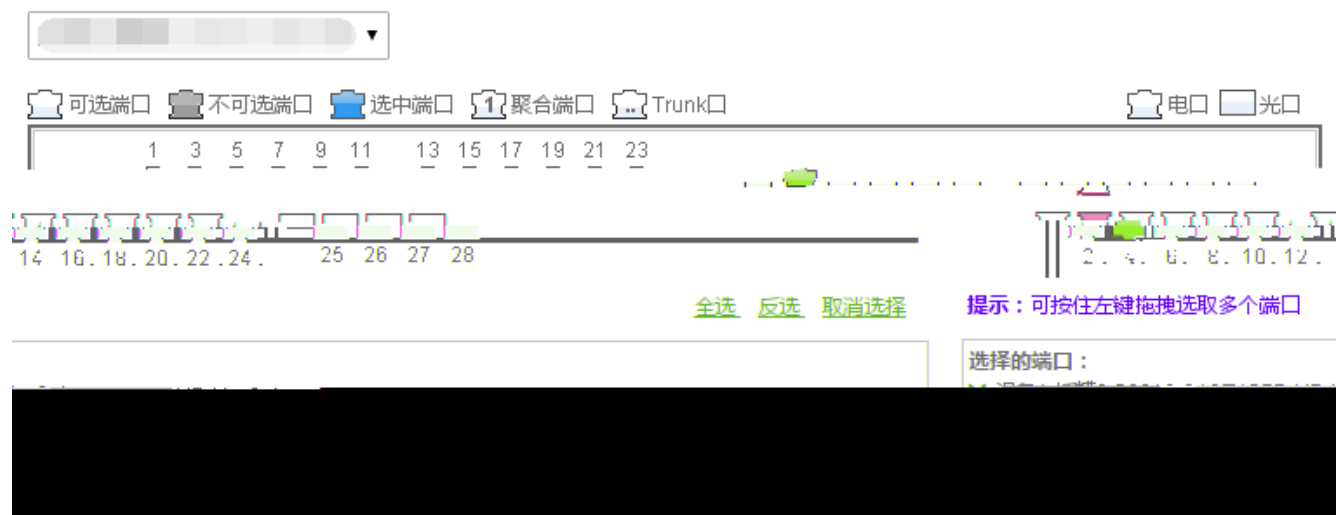
## 1.3 Eweb



/

编辑





WEB

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

	WEB
CWMP	CWMP
	ping      tracet
WEB	CLI

### 1.3.1

1-4

配置

/0/24 管理口：Gi7

VLAN ID: 100 IP: 192.168.182.121

子网掩码: 255.255.255.0

DNS 配置

DNS 服务器: 194.194.194.194

IPv6 地址掩码:

IPv6 网关:

重新设置时间: 2018-05-05 11:05

完成配置 取消

VLAN ID IP

DNS

### 1.3.2

1-5

### 接入诺客MACC平台

正在检测与诺客MACC的连通性，帮助设备与MACC建立连接

本机IP地址：192.168.23.180

默认网关：

DNS服务器：

微信扫一扫如下二维码，根据引导轻松加入诺客MACC管理



IP

DNS

MACC

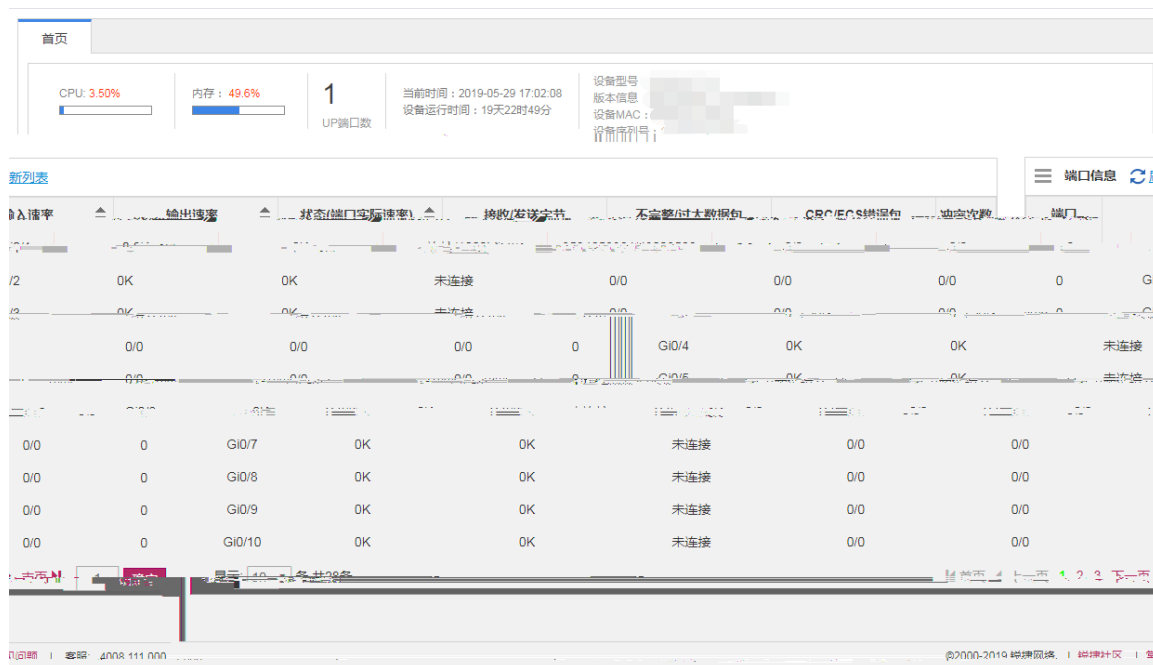
### 1.3.3

VLAN

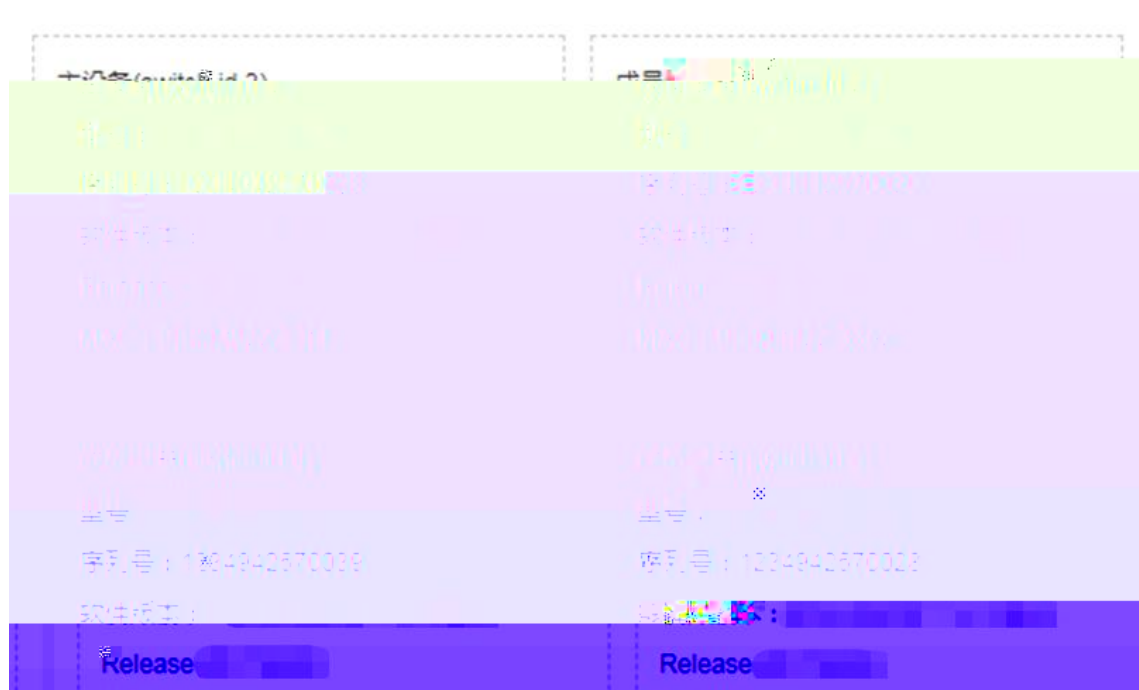
POE

#### 1.3.3.1

1-6



VSU





VLAN设置 Trunk口设置

无Trunk口

Native VLAN: 1 (范围: 1-4094)

允许通过的VLAN: 1-4094 (范围: 3-5,200)

选择端口加入Trunk口: [选择器]

选择的端口:

保存设置 取消

● Trunk

Native Vlan

VLAN(



1-9

+ 批量设置端口 + 添加SVLC

三层端口

端口开关	IP地址	子网掩码	IPv6地址	端口描述	操作	端口
开启	192.168.182.121	255.255.255.0			编辑 删除	Gi7/0/24
					编辑 删除	Vlan 1
Vlan 10	10.0.0.1	255.255.255.0	2001::1/64		编辑 删除	
Vlan 20	20.0.0.1	255.255.255.0	2003::1/64		编辑 删除	
Vlan 30	30.0.0.1	255.255.255.0	2005::1/64		编辑 删除	
Vlan 40	40.0.0.1	255.255.255.0	2004::1/64		编辑 删除	

二层端口

Permit VLAN	端口描述	操作	端口	端口开关	端口类型	Access VLAN	Native VLAN
		编辑 删除	Gi7/0/24	开启			



< >

< >



1-10

端口设置

聚合端口

端口镜像

端口限速

### 三 全局配置

说明：根据设置的流量平衡算法进行流量分配

流量平衡算法：

保存设置

恢复默认值

### 三 聚合配置

说明：将指定端口带宽或实际带宽的聚合命令与多个物理口（成员口）绑定成二层聚合口（聚合口）。每个聚合口最多可以绑定64个成员口，成员口之间通过全互联或

新增聚合口

聚合端口名：

端口类型： 二层口(交换口)  三层口(路由口)

选择端口加入聚合口：

可选端口  不可选端口  选中端口  聚合端口



28

[全选](#) [反选](#) [取消选择](#)



提示：可按住左键拖拽选取多个端口

选择的端口：

! ARP ARP MAC VLAN

< > < >



1-11

端口设置 聚合端口 端口镜像 端口限速

说明：开启端口镜像功能，源端口上的所有报文都会被复制一份转发给目的端口，目的端口上通常连接一个报文分析器分析源端口的报文情况，可以将多个端口镜像到一个目的端口。  
提示：目的端口和源端口不能为同一个。

请选择源端口： (允许选择多个端口，源端口过多可能会影响设备性能)

可选端口 不可选端口 选中端口 聚合端口 电口 光口

提示：可按住左键拖拽选取多个端口 全选 反选 取消选择

选择的端口：  
X 设备1 插槽0 S2910-24GT4SFP-UP-H : 15, 17

请选择目的端口： (只能选择一个端口)

可选端口 不可选端口 选中端口 聚合端口 电口 光口

取消选择

选择的端口：  
X 设备1 插槽0 S2910-24GT4SFP-UP-H : 13

新 配置镜像 删除镜像 刷新

web

< >



< >





端口	POE状态	是否上电	最大功率	分配功率	当前功率	优先级	非标模式	操作
Fa0/1	开启	否	N/A	3.0W	0.0W	低	关闭	编辑
Fa0/2	开启	否	N/A	10.0W	0.0W	低	关闭	编辑
Fa0/3	开启	否	N/A	30.0W	0.0W	低	关闭	编辑
Fa0/4	开启	否	N/A	10.0W	0.0W	低	关闭	编辑
Fa0/5	开启	否	N/A	10.0W	0.0W	低	关闭	编辑
Fa0/6	开启	否	N/A	10.0W	0.0W	低	关闭	编辑
Fa0/7	开启	否	N/A	10.0W	0.0W	低	关闭	编辑
Fa0/8	开启	否	N/A	0.0W	0.0W	低	关闭	编辑

显示: 10 条 共8条

首页 < 上一页 1 下一页 > 末页 确定

Poe

&lt;

&gt;

&lt; &gt;

&lt;

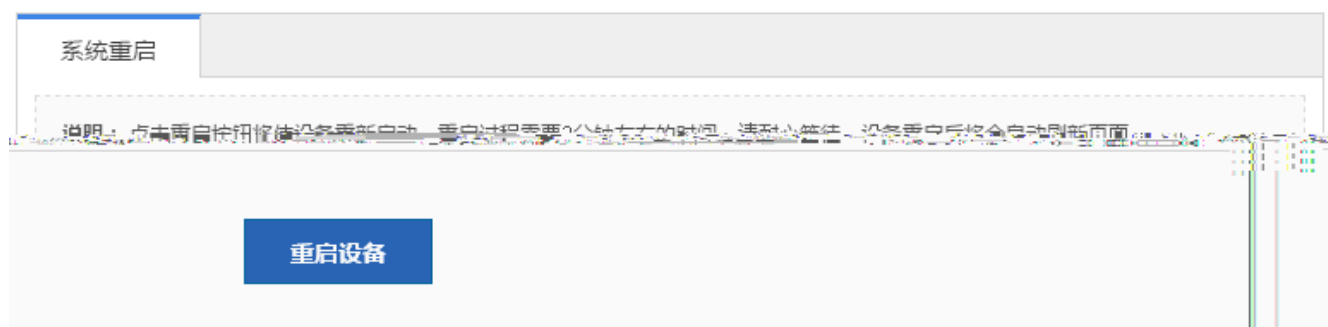
&gt;

1-14

POE端口设置	全局设置
<p>可用总功率：125.0 W</p> <p>剩余总功率：125.0 W</p> <p>供电管理模式：自动模式</p> <p>保存设置</p>	

### 1.3.3.5

1-15



### 1.3.4

MAC

IGMP

DHCP

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

+ 添加静态地址    X 删除静态地址

端口	MAC地址	VLAN ID	操作
GigabitEthernet 1/0/8	2244.1234.2562	10	删除

显示: 10 条 共2条    首页   上一页   1   下一页   末页

MAC    VLAN ID

<   >    <   >

2    <   >



1-17

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

0002.0002.0003	4	编辑   删除
----------------	---	---------

1 下一页   末页   1   确定    显示: 10 条 共1条    首页   上一页

MAC VLAN ID

•

< >

< >

•

2

< >

### 1.3.4.2



1

2

## 1.3.4.3

## RLDP



1-19

生成树全局设置	生成树端口设置	RLDP设置
<b>三 全局设置</b>		
生成树开关： <input checked="" type="checkbox"/> ON		
优先级： <input type="text" value="8"/> <small>范围(0-15)，默认8</small>	握手时间： <input type="text" value="2"/> <small>范围(1-10)秒，默认2</small>	
老化时间： <input type="text" value="20"/> <small>范围(6-40)秒，默认20</small>	转发延迟： <input type="text" value="15"/> <small>范围(4-30)秒，默认15</small>	
生成树模式： <input type="text" value="MSTP"/>		
MST名称： <input type="text"/> <small>32字节以内的字符串</small>	MST版本： <input type="text" value="0"/> <small>范围(0-65535)，默认0</small>	
<input type="button" value="保存设置"/>		
<b>三 MST 设置</b>		
<small>说明：添加实例时，建议您先关闭生成树开关，配置好后再打开，以保证网络拓扑的稳定和收敛。</small>		
+ 添加实例    × 删除选中实例		
<input type="text" value="8"/>	<input type="text" value="默认实例，不可编辑"/>	<input type="text" value="0"/>
<input type="text" value="ALL"/>		
MSTP		MST

VLAN

•

< >

< >

•

1

2

< >

0





### 1.3.4.4 IGMP

#### IGMP

##### 1-21 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，从而节省网络带宽。

操作	<input type="checkbox"/>	组策略标识	组播地址	策略动作	策略应用端口
无记录信息					

末页 1 确定      显示: 10 条共0条      首页 上一页 下一页

●

●

●

1

2

### 1.3.4.5 DHCP

#### DHCP

##### 1-22 DHCP

DHCP 中继

给DHCP客户端。

### 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

#### 1.3.4.6

web

web

web

1-23 web

外置web认证

高级设置

说明：上网实名认证是指一种基于Web的认证，是一种对用户访问网络的权限进行控制的身份认证方法，这种认证方法不需要用户安装专用的客户端认证软件，使用普通的浏览器软件就可以进行身份认证。

服务器类型 一认证 二认证

服务器IP地址：  \*重定向主页：  \*认证方法：  ▼ [【管理Radius服务器】](#)记账方法：  ▼SNMP服务器： [【SNMP服务器】](#) \*选中开启认证：   ▼ 电口  光口 可选端口  不可选端口  选中端口  聚合端口

1	3	5	7	9	11	13	15	17	19	21	23
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

   [全选](#) [反选](#) [取消选择](#)

提示：可按住左键拖拽选取多个端口

选择的端口：

X 设备1 插槽0 S2910-24GT4SFP-UP-H : 13-14

清除设置

保存设置

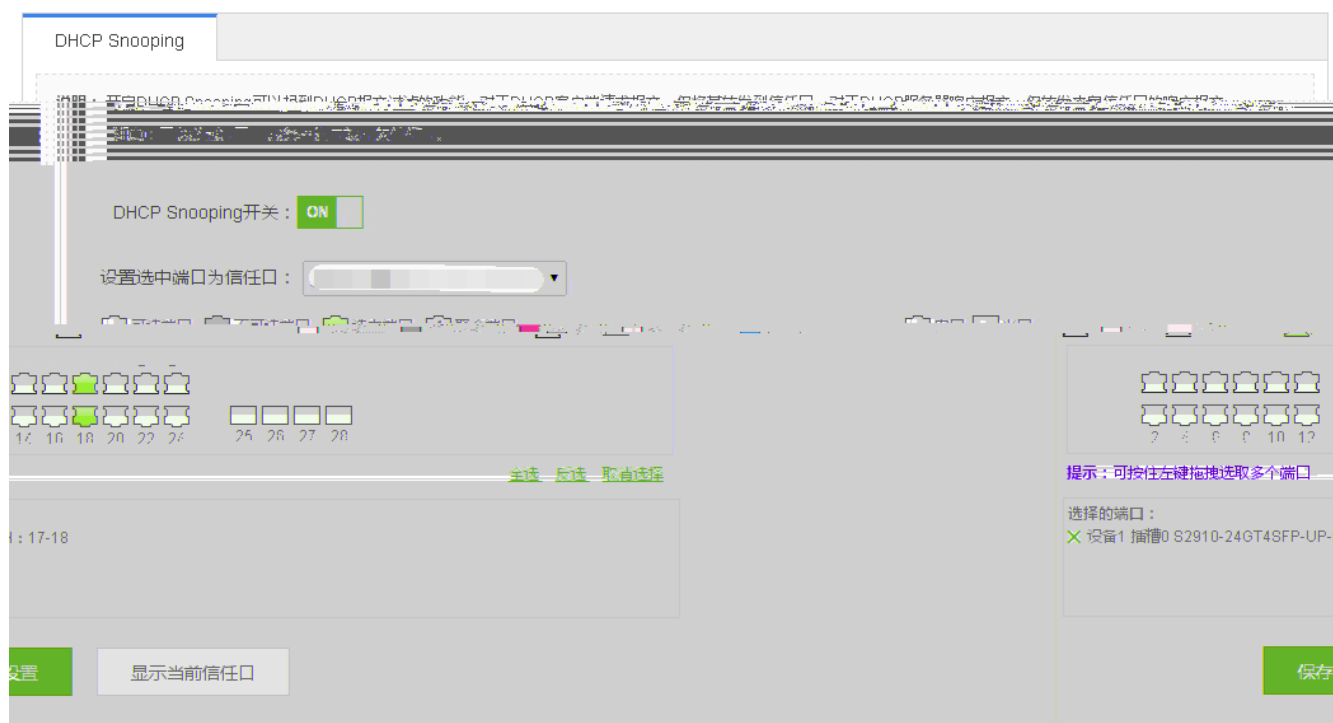
IP



1-24

外置web认证	高级设置
<p>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。</p> <p>置在线用户信息的更新时间间隔。</p> <p>范围:1-65535) 多个用“ ”隔开，最多可配置10个。</p>	
重定向超时时间：	<input type="text" value="3"/> (范围:1-10秒，默认3) 设置维持
在线信息更新时间：	<input type="text" value="180"/> (范围:30-3600秒，默认180) 设置
重定向HTTP端口：	<input type="text" value="80"/> (端口号)
<p>IP地址：<input type="text"/> 掩码：<input type="text"/> <input type="button" value="X"/> <input type="button" value="+添加"/></p> <p>免认证用户IP：该用户可以直接上网，不需要认证,最大允许配置50条规则。</p> <p>IP地址：<input type="text"/> 掩码：<input type="text"/> <input type="button" value="X"/> <input type="button" value="+添加"/></p> <p><input type="button" value="保存设置"/> <input type="button" value="清除设置"/></p>	

### 1.3.5



DHCP SERVER  
DHCP

DHCP

DHCP SERVER  
< >

### 1.3.5.2 ARP

ARP

ARP

ARP

DAI

ARP



防网关ARP欺骗    ARP检查设置    DAI设置    ARP表项

说明：防止客户端冒充网关发送网关地址的ARP请求。只在指定主机的端口配置。上联接口不用配置。

+ 添加过滤端口    X 删除选中的过滤端口

操作	过滤端口	IP
		无记录信息

上一页 下一页 ▶ 末页 ▶▶  确定

显示:  条 共0条    ◀ 首页 ▶

- 
- 
- 
- 1
- 2

IP

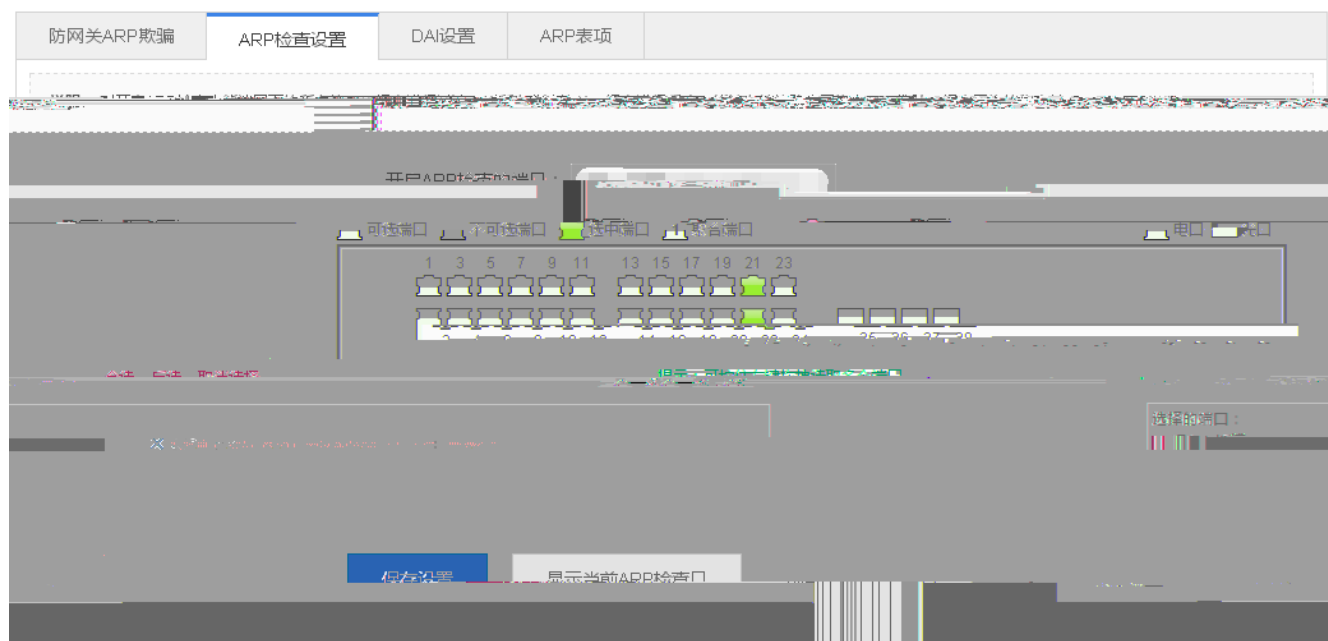
< >

< >

< >

## ARP

1-27 ARP



### ARP

- ⓘ ARP
- < ARP > ARP
- ⚠ DHCP Snooping ARP
- ↙ DAI
- 1-28 DAI

防网关ARP欺骗    ARP检查设置    **DAI设置**    ARP表项

### 三 VLAN DAI设置

说明：在打开DAI检查功能的VLAN所对应的非信任端口上启用所有ADD请求和动态学习，对所有非法的ADD请求进行丢弃。

开启DAI的VLAN：[【删除全部VLAN DAI设置】](#)

VID3    [X 批量删除](#)

### 三 DAI信任口

说明：从信任端口接收到的报文将跳过DAI检查，被认为是合法的ARP报文。

【设备端口】：

端口  电口  光口

21	23
22	24
25	26
27	28

可选端口     不可选端口     选中端口     聚合口

1	3	5	7	9	11	13	15	17	19
2	4	6	8	10	12	14	16	18	20

[全选](#)    [反选](#)    [取消选择](#)

选择的端口：

设备1 插槽0 S2910-24

[保存设置](#)

[查看当前DAI信任口](#)

1 VLAN DAI

DAI VLAN

2 DAI

DAI



DAI



DAI



DAI



DHCP Snooping

ARP

### 三 ARP

1-29 ARP

防网关ARP欺骗		ARP检查设置		DAI设置		ARP表项	
<a href="#">动态&gt;&gt;静态绑定</a> <a href="#">解除静态绑定</a> <a href="#">手工绑定</a>		基于IP地址查询：		<input type="text"/>		<a href="#">搜索</a>	
<input type="checkbox"/>	IP地址	MAC地址	类型	操作			
<input type="checkbox"/>	172.18.124.1	1414.4b72.fa9b	动态绑定	<a href="#">动态&gt;&gt;静态绑定</a>			
<input type="checkbox"/>	172.18.124.17	b8ac.6f40.50e8	动态绑定	<a href="#">动态&gt;&gt;静态绑定</a>			
<input type="checkbox"/>	172.18.124.52	b8ac.6f3e.fa9c	动态绑定	<a href="#">动态&gt;&gt;静态绑定</a>			
<input type="checkbox"/>	172.18.124.55	6c62.6dd2.f4f3	动态绑定	<a href="#">动态&gt;&gt;静态绑定</a>			
<input type="checkbox"/>	172.18.124.66	0026.9e04.f9fb	动态绑定	<a href="#">动态&gt;&gt;静态绑定</a>			
<input type="checkbox"/>	172.18.124.73	00d0.f822.3441	本设备接口ARP表项	<a href="#">动态&gt;&gt;静态绑定</a>			
<input type="checkbox"/>	172.18.124.132	0024.2178.20e1	动态绑定	<a href="#">动态&gt;&gt;静态绑定</a>			
<a href="#">首页</a> <a href="#">&lt; 上一页</a> <a href="#">1</a> <a href="#">下一页 &gt;</a> <a href="#">末页</a>		<input type="text" value="1"/> <a href="#">确定</a>		显示 <input type="text" value="10"/> 条共 8条			

- >>

1 ARP

2 ARP < >

- 

1 ARP

2 ARP < >

- 

IP MAC

ARP

### 1.3.5.3 IP Source Guard

IP Source Guard



1-30



- 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 < >



1-31



-



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，防止黑客对数网进行IP扫描占用带宽。设备每秒处理报文 **不超过4个**。  
[【IP防扫描列表】](#)

[【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。

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】](#)

### 1.3.5.6

1-35

风暴控制

+ 添加风暴控制端口 × 删除选中的风暴控制端口

端口	广播	组播	未知单播	操作	接口
-	-	-	-	编辑 删除	Gi1/0/1
50%	60%	70%	-	编辑 删除	Gi1/0/2
-	-	-	-	编辑 删除	Gi1/0/3
-	-	-	-	编辑 删除	Gi1/0/4
-	-	-	-	编辑 删除	Gi1/0/5
-	编辑 删除	Gi1/0/6	-	-	-
-	-	-	编辑 删除	-	Gi1/0/8
-	-	-	编辑 删除	-	Gi1/0/9
-	编辑 删除	Gi1/0/10	-	-	-

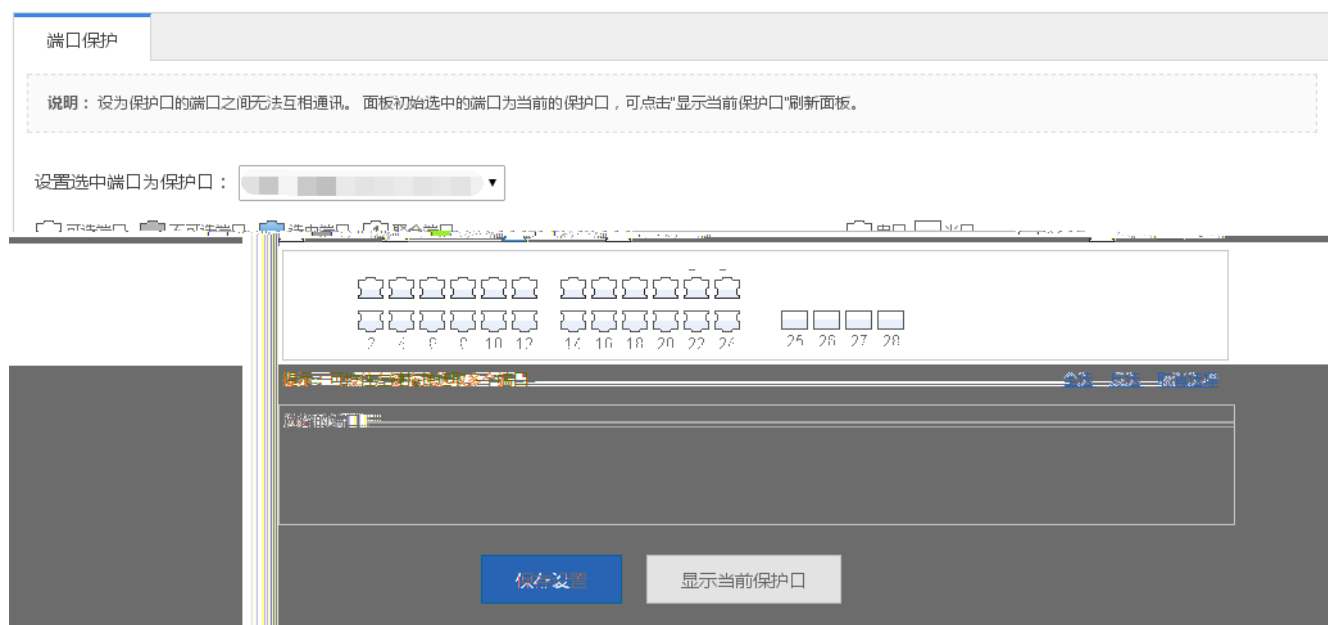
首页 < 上一页 1 2 3 4 5 下一页 > 末页 | 1 确定 显示: 10 条 共56条

- 
- 
- < >
- >
- 
- 1
- 2 < >

### 1.3.6

#### 1.3.6.1

1-36



### 1.3.6.2 DHCP

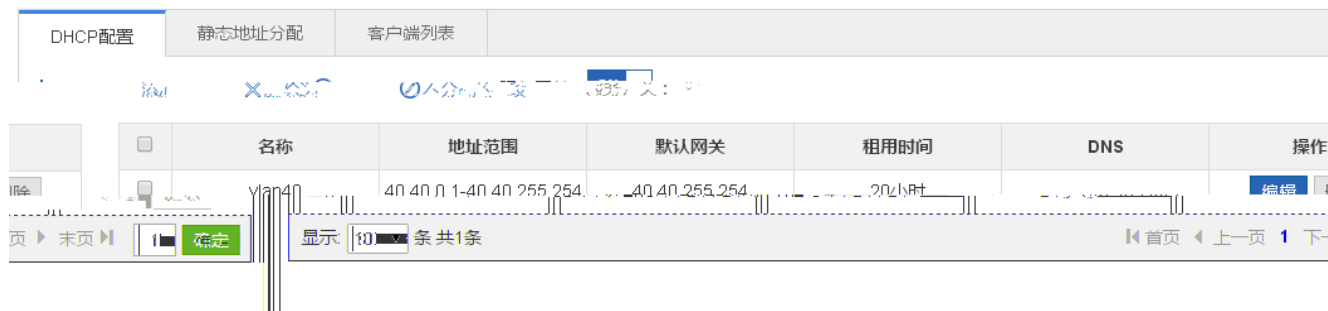
DHCP

DHCP

DHCP

DHCP

1-37 DHCP



- DHCP

IP

DHCP

- DHCP

DHCP

< >

DHCP

< >

● DHCP

1 DHCP

DHCP

2 DHCP

< >

DHCP

● DHCP

<DHCP

>

DHCP



1-38

DHCP

静态地址分配

静态地址列表

+ 添加静态地址 X 删除选中地址

客户名称	客户IP	掩码	网关	客户端MAC	DNS服务器	操作
无记录信息						

一页 下一页 末页 1 确定 显示: 10 条共0条 首页 上

●

IP

MAC

●

< >

< >

●

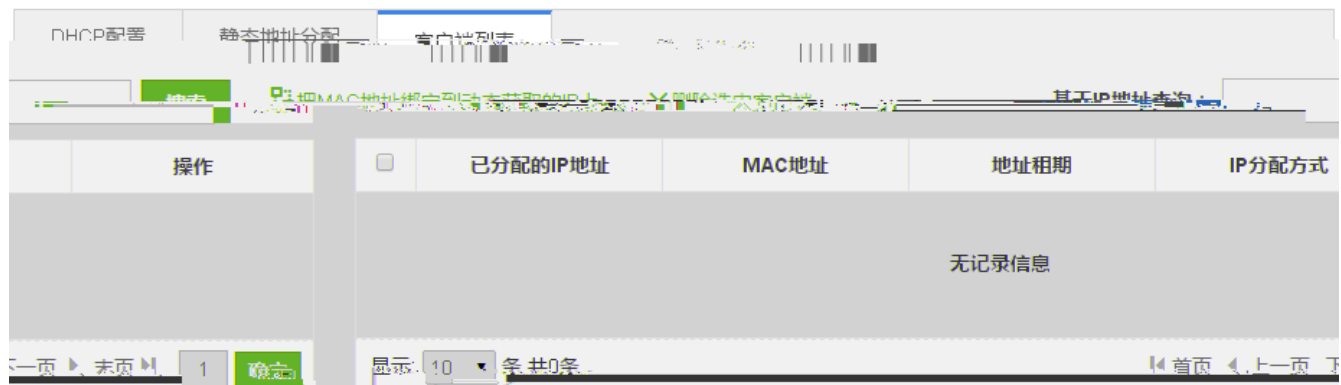
1

2

< >



1-39



- IP

- IP

- MAC

- IP

- MAC

- IP

### 1.3.6.3 ACL

#### ACL

ACL

1-40ACL



- ACL

- ACL

- ACL

- ACL

ACL

IP

ACL

● ACL

ACL

< >

ACL

<

>

● ACL

1 ACL

2 ACL

< >

● ACL

ACL

ACL

ACL

1-41 ACL

ACL列表	ACL时间	应用ACL
-------	-------	-------

时间段	操作	时间对象	时间周期
8:00-16:00	<a href="#">编辑</a> <a href="#">删除</a>	worktime	工作日

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

● ACL

ACL

ACL

● ACL

ACL

< >

ACL

<

>

● ACL

ACL

ACL

ACL

1-42 ACL



- ACL
- ACL ACL ACL ACL
- ACL
- ACL < > ACL ACL <
- >
- ACL
- 1 ACL ACL
- 2 ACL < >

### 1.3.6.4 QOS



1-43



- ACL
-

< >

< >



1

2

< >



1-44

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

策略名称	策略描述	策略动作	策略生效时间	策略生效范围
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



< >



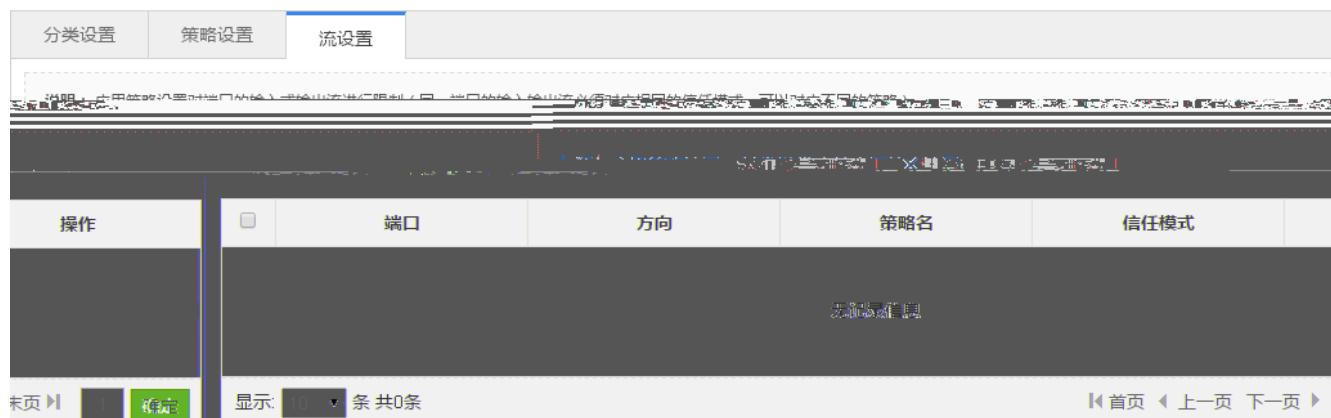
< >

< >



1

1-45



●

●

1

< >

2

< >

### 1.3.7

CWMP

Web

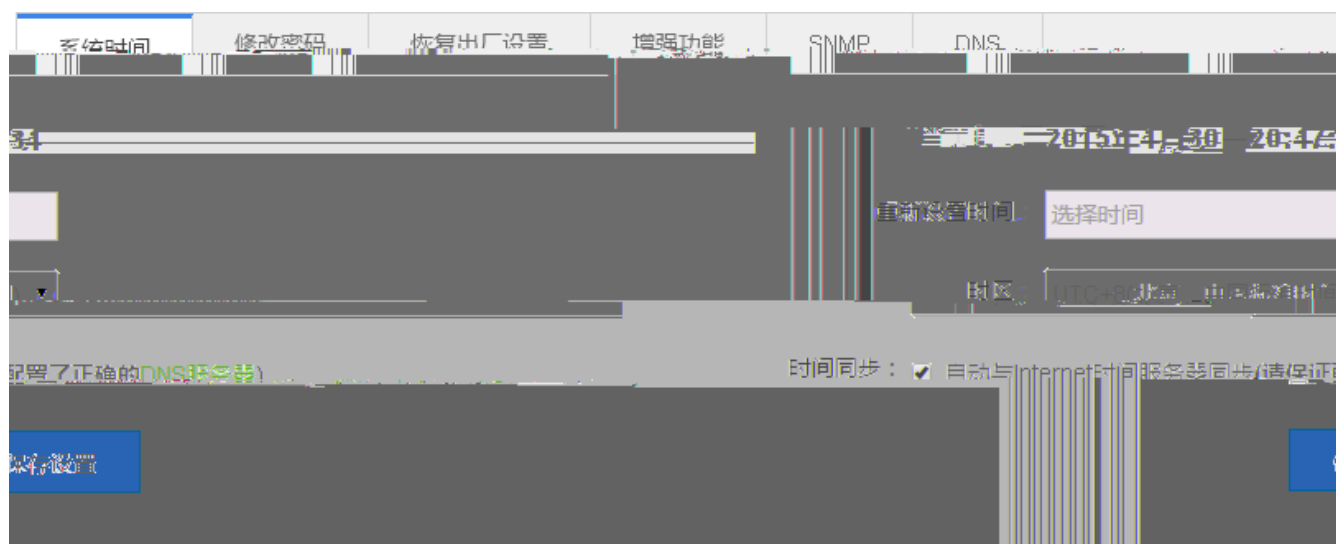
#### 1.3.7.1

SNMP

DNS



1-46



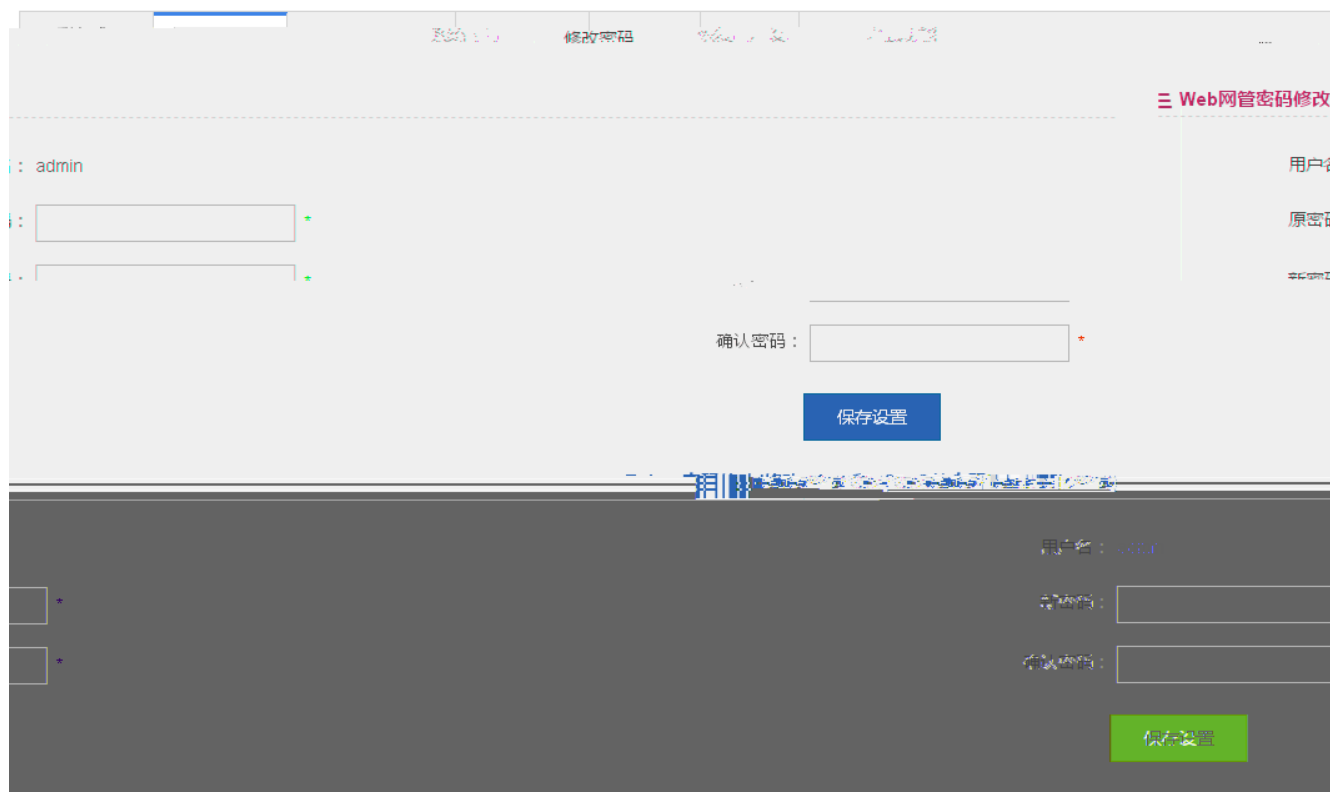
- 

Internet

< >



1-47



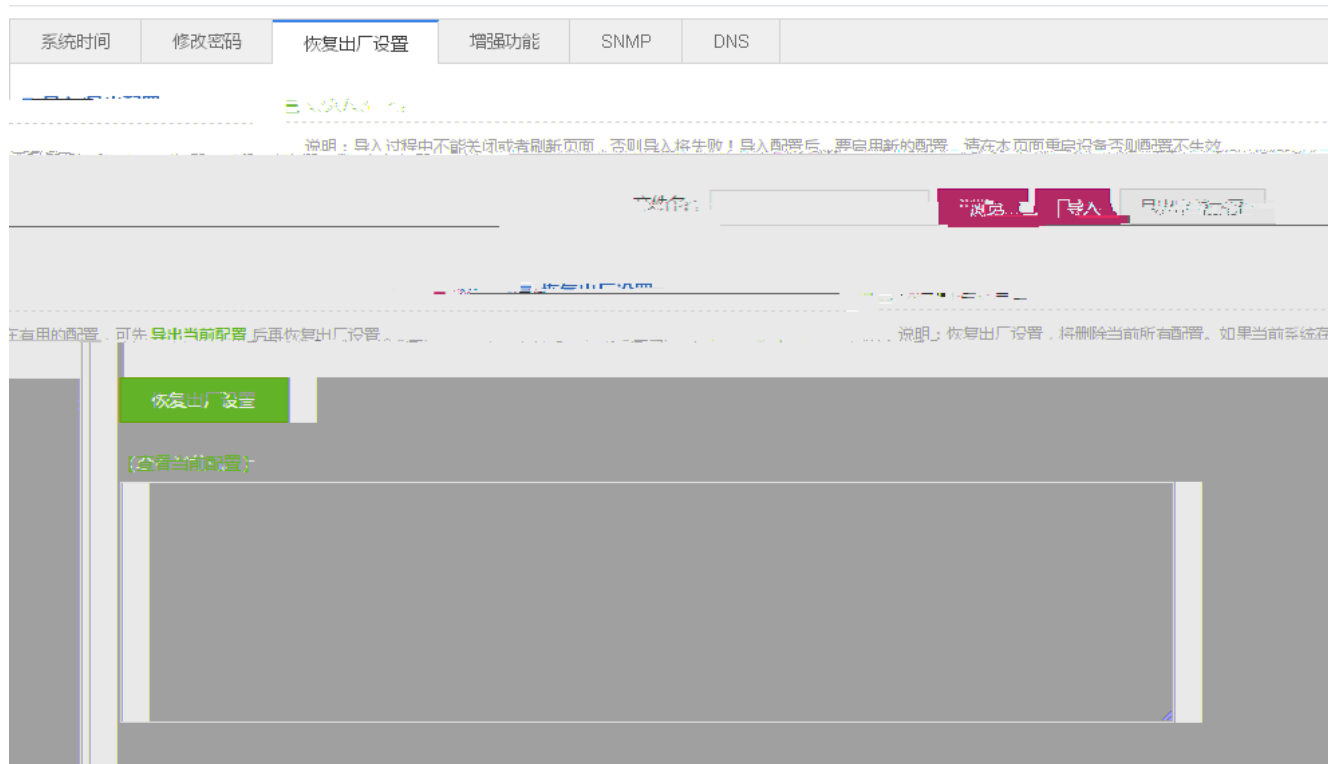
● Web

Web

< >

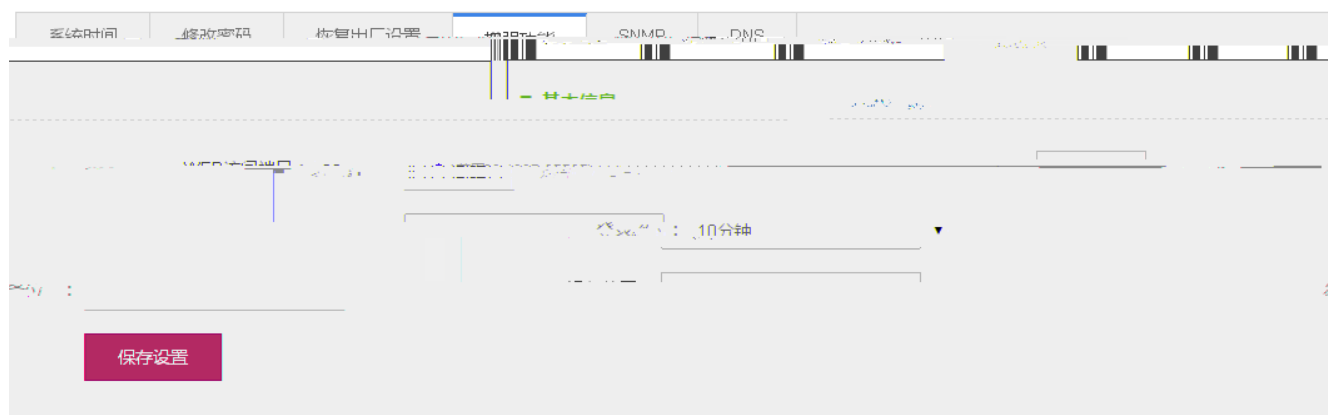


web



- /
- 
- < >
- ↓

1-49





### 1.3.7.2

1-54

日志服务器
查看系统日志

系统日志 ( show log )
更新当前系统日志

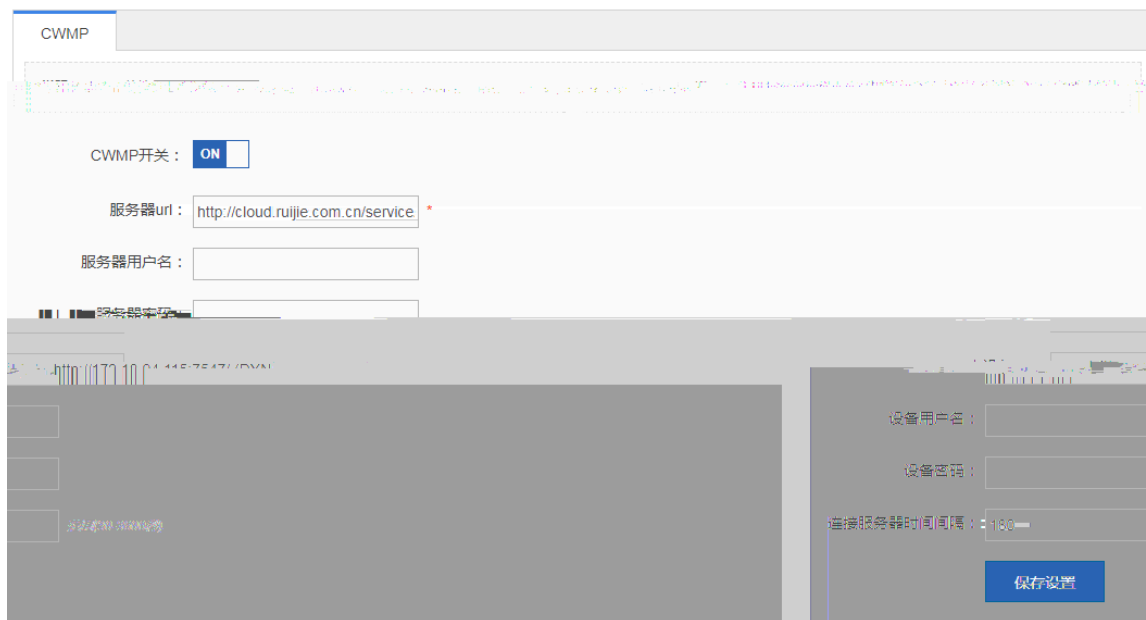
```

Syslog logging: disabled
  Console logging: level debugging, 659 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 659 messages logged
  Standard format:false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: disable
  Sysname log messages: disable
  Count log messages: disable
  Trap logging: level informational, 0 message lines logged,0 fail
Log Buffer (Total 131072 Bytes): have written 47225,
*Jan  1 08:00:34: %LOCAL_DP-5-LC_PROB: Board information in this chassis has been collected.
*Jan  1 08:00:34: %SWITCH-6-INSTALL: Install chassis ES224 on switch 1
*Jan  1 08:00:34: %DP-6-MASTER: Module in slot 6 has translated to master...
*Jan  1 08:00:39: %DEV_MONITOR-4-CARD_POWER_ON: The power enough card in slot 4 will be controlled to power on automatically.
*Jan  1 08:00:45: %DP-5-PROB: Board probing has completed.
*Jan  1 08:00:45: %DEV_MONITOR-3-DEFINES_INIT: ...

```

### 1.3.7.4 CWMP

CWMP



CWMP

CWMP

url

url

### 1.3.7.5

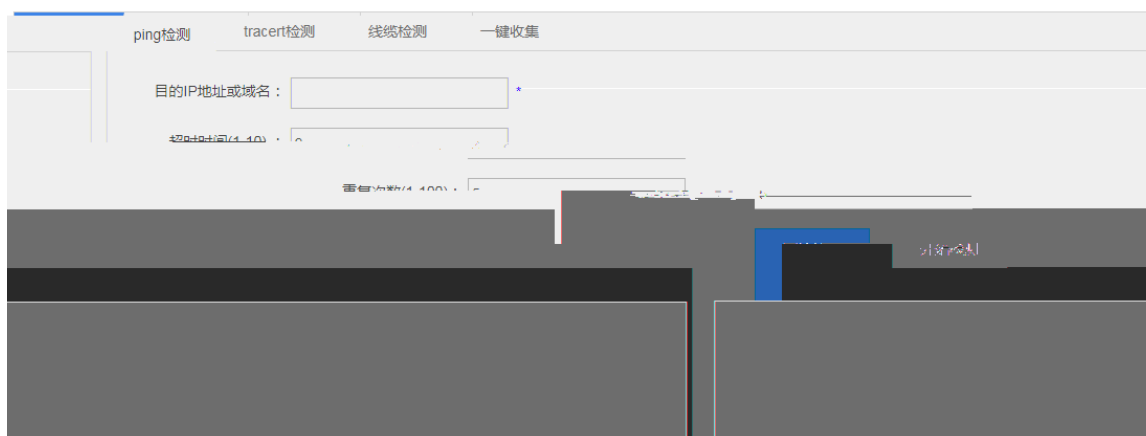
ping

tracert

#### Ping

Ping

1-55 ping



IP

<

>

#### tracert

## tracert

## 1-56 tracert

ping检测    **tracert检测**    线缆检测    一键收集

目的IP地址或域名：

超时时间(1-10)：

**开始检测**

ping

IP

&lt;

&gt;



## 1-57

ping检测    tracert检测    **线缆检测**    一键收集

说明：百兆口仅检测A和B两对纤芯，长度误差10米

选择端口：

可选端口   
 不可选端口   
 选中端口   
 聚合端口   
 电口   
 光口

[取消选择](#)

**开始检测**

&lt;

&gt;

&lt;

&gt;

## 1-58

ping检测    tracert检测    **线缆检测**    一键收集

选择端口：

取消选择

检测结果：

端口:(A/B/C/D分别代表网线4对芯)	状态	长度
G10/19:A	断路	0
G10/19:B	断路	0
G10/19:C	断路	0
G10/19:D	断路	0



1-59

ping检测    tracert检测    **线缆检测**    一键收集

说明：一键收集将收集设备的故障信息，便于排查设备故障。

**一键收集**

### 1.3.7.6 WEB

CLI  
?

CLI

TAB

