

WEB

I > \$15. ' ' ?

S5700H_IRGOS11.4(1)B42

V(%

cf gyr`^_t ©)' (/

copyright © 2018





/

3.

1 Eweb

1.1

IE WEB
WEB WEB WEB WEB IE WEB
WEB WEB



S57H

1.2

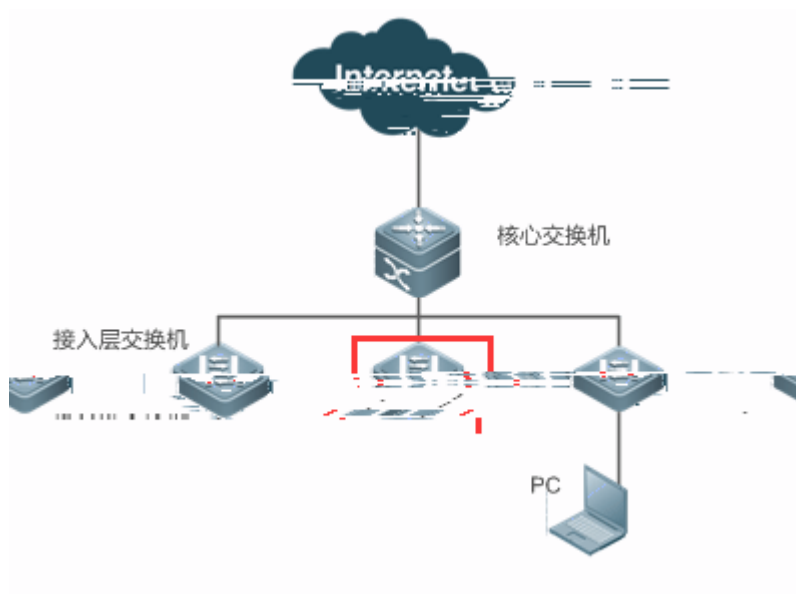
<u>WEB</u>	WEB
------------	-----

1.2.1 WEB

PC

WEB

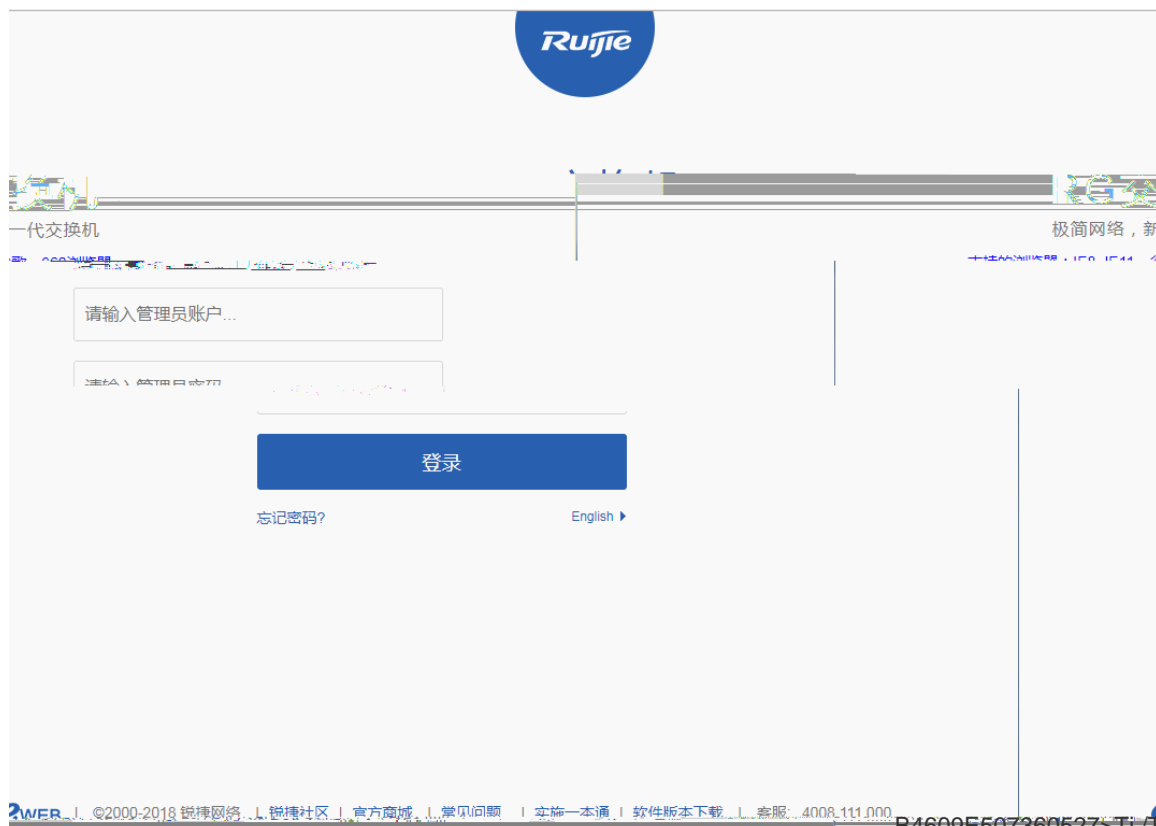
1-1



PC ping

WEB





B4609E507360527>Tj/TT1372.6()Tj 04080379>Tj /TT3

修改密码

用户名： admin

新密码：

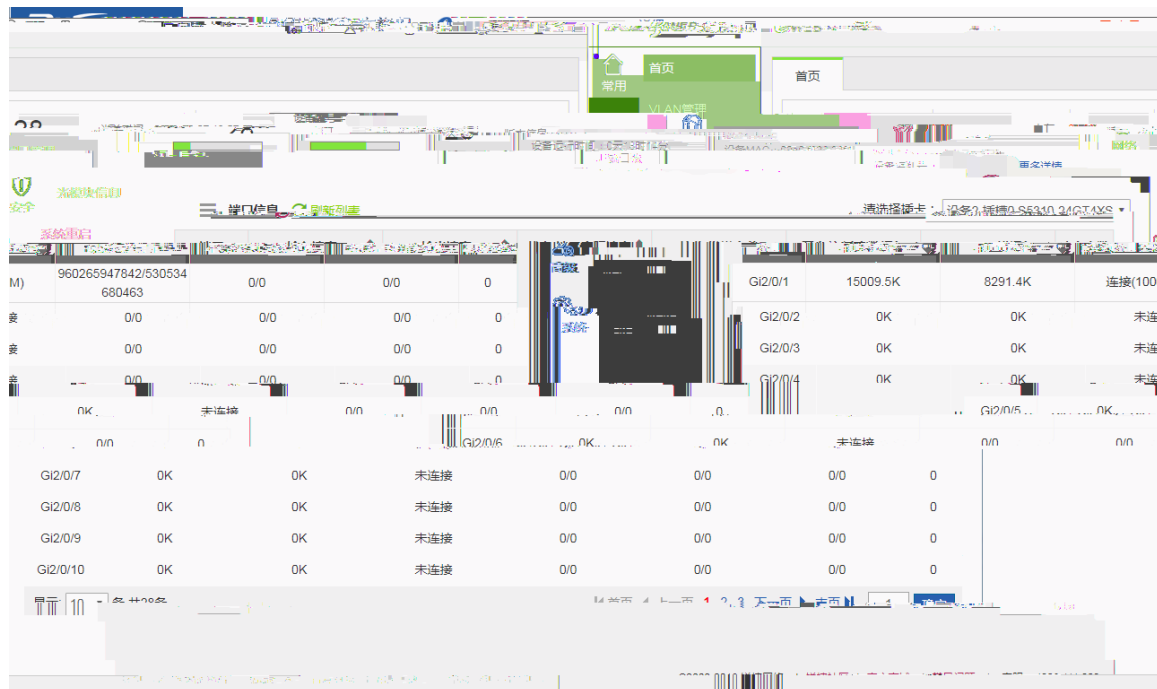
确认密码：

当前密码为默认密码，为提高系统的安全性，请修改密码

WEB

WEB









1-3 WEB




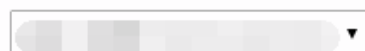
Eweb

Eweb

1.3 Eweb

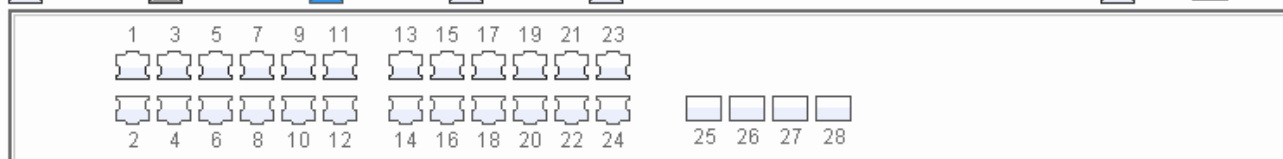
/	
	
	
	
	
	
	
	Trunk VLAN /VLAN
	

	
	
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
  Trunk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：

< >

< >

< >

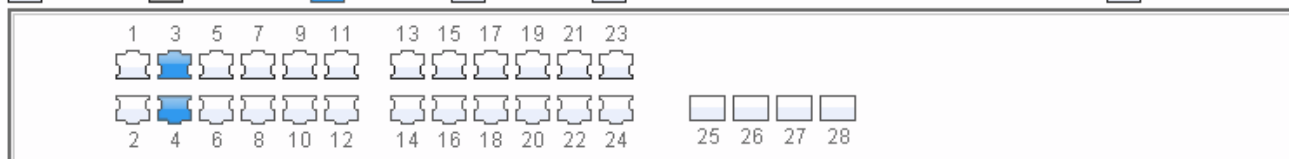
< >

< >



可选端口
 不可选端口
 选中端口
 聚合端口
 Trunk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：

✕ 设备1 插槽0 S2910-24GT4SFP-UP-H : 3-4

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
ACL	ACL ACL ACL
QOS	

SNMP

1.3.2

VLAN

POE

1.3.2.1

1-5

端口	速度	连接	MAC地址	其他参数
G12/0/1	13431K	7422.1K	连接(1000M)	942377631518/520647287 120
0	G12/0/3	OK	OK	未连接
0	G12/0/4	OK	OK	未连接
0	G12/0/5	OK	OK	未连接
0	G12/0/6	OK	OK	未连接
0	G12/0/7	OK	OK	未连接
0	G12/0/8	OK	OK	未连接
0	G12/0/9	OK	OK	未连接
0	G12/0/10	OK	OK	未连接

显示 10 条 共28条

VSU



1.3.2.2 VLAN

VLAN VLAN Trunk

VLAN

VLAN

1-6 VLAN





1.3.2.3

1-8





1-9

端口设置 **聚合端口** 端口镜像 端口限速

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：

聚合口设置

说明：为了在端口聚合或实现负载均衡，将多个物理端口（成员口）绑定成一个逻辑口（聚合口），每个聚合口最多可以绑定64个成员口。成员口间通过广播地址和组播地址进行通信。



< >
< > < >

< >
< > < >



ARP

ARP

MAC VLAN

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](#) [X 批量删除限速端口](#)

输出速率(Kbps)	操作	端口	输入速率(Kbps)
10000	配置 删除	Gi1/0/7	10000
	配置 删除	Gi1/0/9	100000
	配置 删除	Gi1/0/11	100000

首页 < 上一页 1 下一页 > 末页

< >

< >

光模块信息

说明：当出现接收发送光功率过高或过低时请查看下光纤线缆是否异常。

选择端口：存在光模块

接口	状态	光模块类型	接口类型	中心波长(nm)	光纤传输距离	DDM	SN	接收光功率	发送光功率
Te20/26	正常	10GBASE-SR	No scorable connector	1310	100m(Cable)	YES	13100000000000000000	-20.01dBm	1.02
Te20/27	正常	10GBASE-SR	No scorable connector	1310	100m(Cable)	YES	13100000000000000000	-20.01dBm	1.02
Te20/28	正常	10GBASE-SR	No scorable connector	1310	100m(Cable)	YES	13100000000000000000	-20.01dBm	1.02
Te20/29	正常	10GBASE-SR	No scorable connector	1310	100m(Cable)	YES	13100000000000000000	-20.01dBm	1.02

1.3.2.5 POE

POE

1-14



1.3.2.6

1-15



<

>

<

>

1.3.3

MAC

IGMP

DHCP

1.3.3.1 MAC

MAC

1-16

静态地址设置

说明

在交换机转发数据时，需要根据MAC地址来做出相应转发。手工方式指定设备下接的网络设备的MAC地址与端口关系，即添加一个静态地址。当在VLAN中接收到的地址与该地址一致时，即转发到指定的端口。

[+ 添加静态地址](#) [X 删除静态地址](#)

MAC地址	VLAN ID	操作
2244.2266.6622	2	删除
2244.1234.2562	10	删除

◀ 首页 ◀ 上一页 1 下一页 ▶ 末页 ▶ 1 确定

<input type="checkbox"/>	端口
<input type="checkbox"/>	GigabitEthernet 1/0/9
<input type="checkbox"/>	GigabitEthernet 1/0/8

显示: 10 条 共2条

MAC VLAN ID

< >

< >

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

< >

< >

2

< >

1.3.3.2

1-18

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

<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



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(10-500)秒，默认300

桥置标志： 范围(0-FFFF)十六进制，默认0000

生成树模式：

保存设置

三 MST 设置

+ 添加实例 X 删除选中实例

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

MSTP

MST

VLAN

< > <

生成树全局设置		生成树端口设置	RLDP设置				
+ 批量设置							
说明：建议直连PC的端口开启Port Fast							
端口	端口状态	Port Fast	BPDU Guard	保护模式	连接类型	实例/端口优先级	操作
编辑	Gi2/0/24	关闭	关闭	关闭	关闭	point-to-point	0 0 128
编辑	Gi2/0/23	关闭	关闭	关闭	关闭	point-to-point	0 0 128
编辑	Gi2/0/22	关闭	关闭	关闭	关闭	point-to-point	0 0 128
编辑	Gi2/0/21	关闭	关闭	关闭	关闭	point-to-point	0 0 128
编辑	Gi2/0/20	关闭	关闭	关闭	关闭	point-to-point	0 0 128
编辑	Gi2/0/19	关闭	关闭	关闭	关闭	point-to-point	0 0 128
编辑	Gi2/0/18	关闭	关闭	关闭	关闭	point-to-point	0 0 128
	关闭	关闭	关闭	point-to-point	0 0 128	Gi2/0/17	关闭
	关闭	关闭	关闭	point-to-point	0 0 128	Gi2/0/16	关闭
	关闭	关闭	关闭	point-to-point	0 0 128	Gi2/0/15	关闭
首页 上一页 1 2 3 4 5 下一页 末页						显示: 10 条 共48条	

Port Fast BPDU

< >

< >

RLDP

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](#)

1 RLDP

RLDP

RLDP

< >

2 RLDP

RLDP

RLDP

RLDP

RLDP

RLDP

< >

RLDP

< >

RLDP

RLDP

1.3.3.4 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				

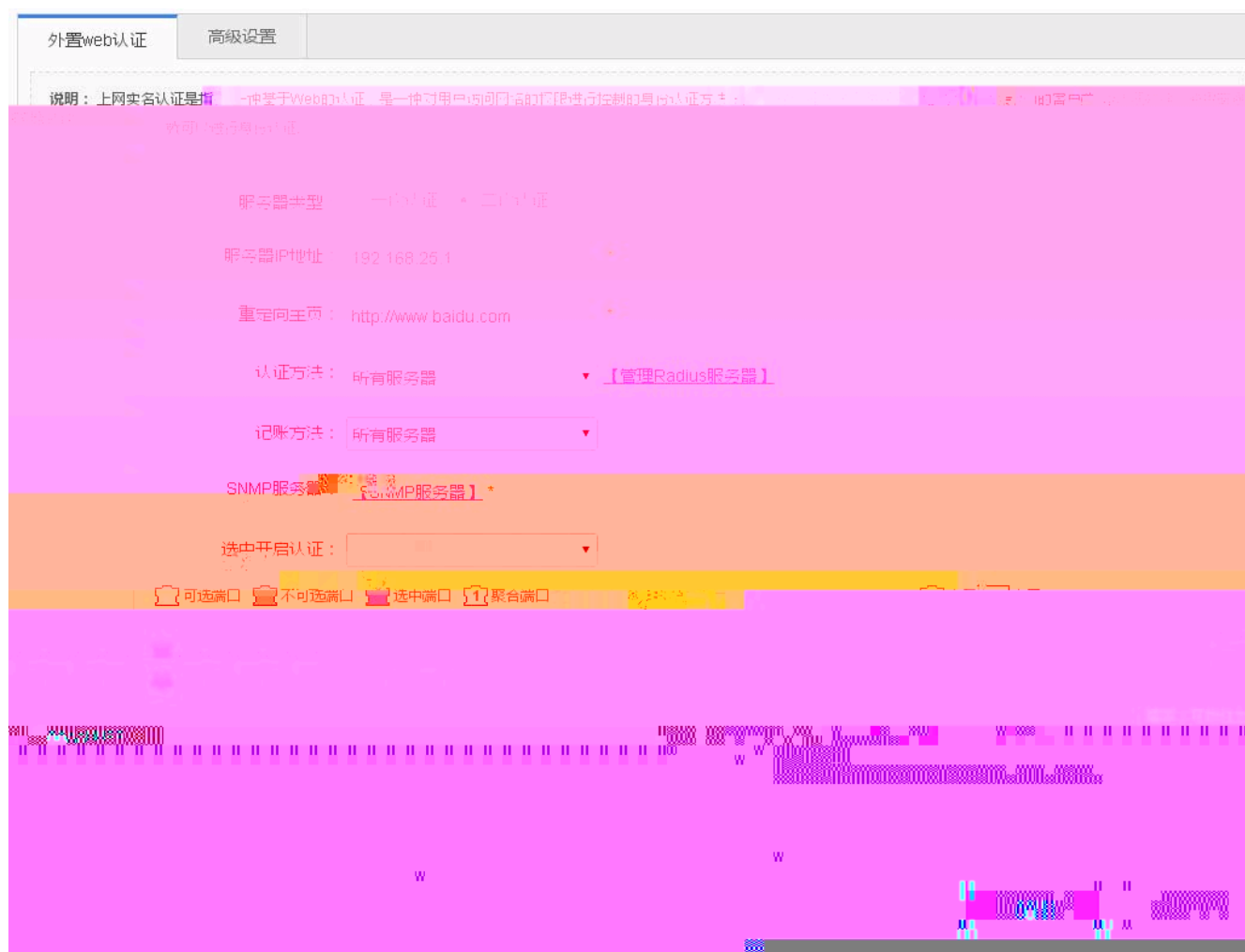
显示: 10 条共0条 ◀ 首页 < 上一页 下一页 ▶ 末页 ▶▶ 1 确定

1.3.3.5

web



1-22 web



IP

1-23

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)	
会话信息更新时间： <input type="text" value="100"/> (范围00-99999)	
重定向HTTP端口： <input type="text" value="80"/>	

1.3.4

DHCP Snooping

ARP

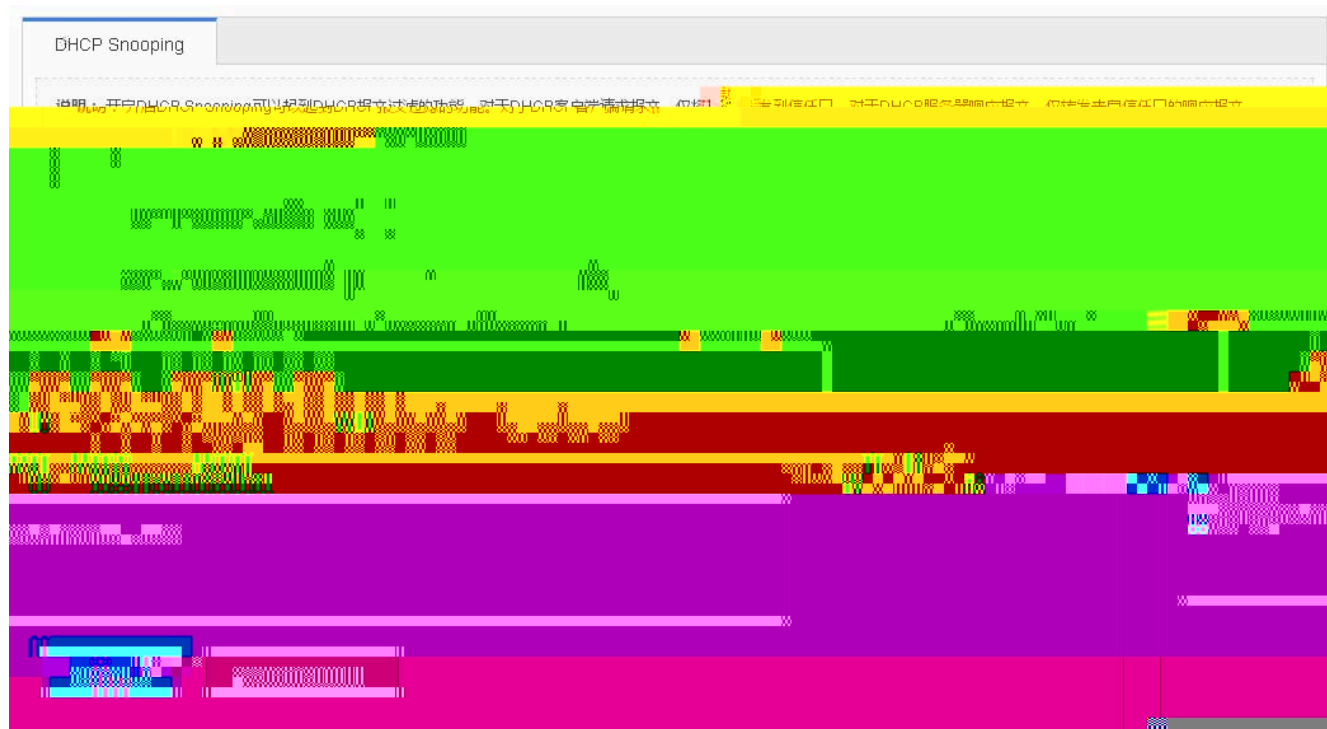
IP Source Guard

NFPP

1.3.4.1 DHCP Snooping

DHCP Snooping

1-24 DHCP Snooping



DHCP SERVER DHCP DHCP SERVER
DHCP < >

1.3.4.2 ARP

ARP ARP ARP DAI ARP

ARP

1-25 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报文，只在接客户机的端口配置，上联接口不用配置。

+ 添加过滤端口 × 删除选中的过滤端口

<input type="checkbox"/>	过滤端口	IP	操作
无记录信息			
显示: <input type="text" value="10"/> 条 共0条 ⏪ 首页 ◀ 上一页 下一页 ▶ 末页 ⏩ <input type="text" value="1"/> <input type="button" value="确定"/> 			

IP

< >

< >

1

2

< >

ARP




1-26 ARP


防网关ARP欺骗 **ARP检查设置** DAI设置 ARP表项

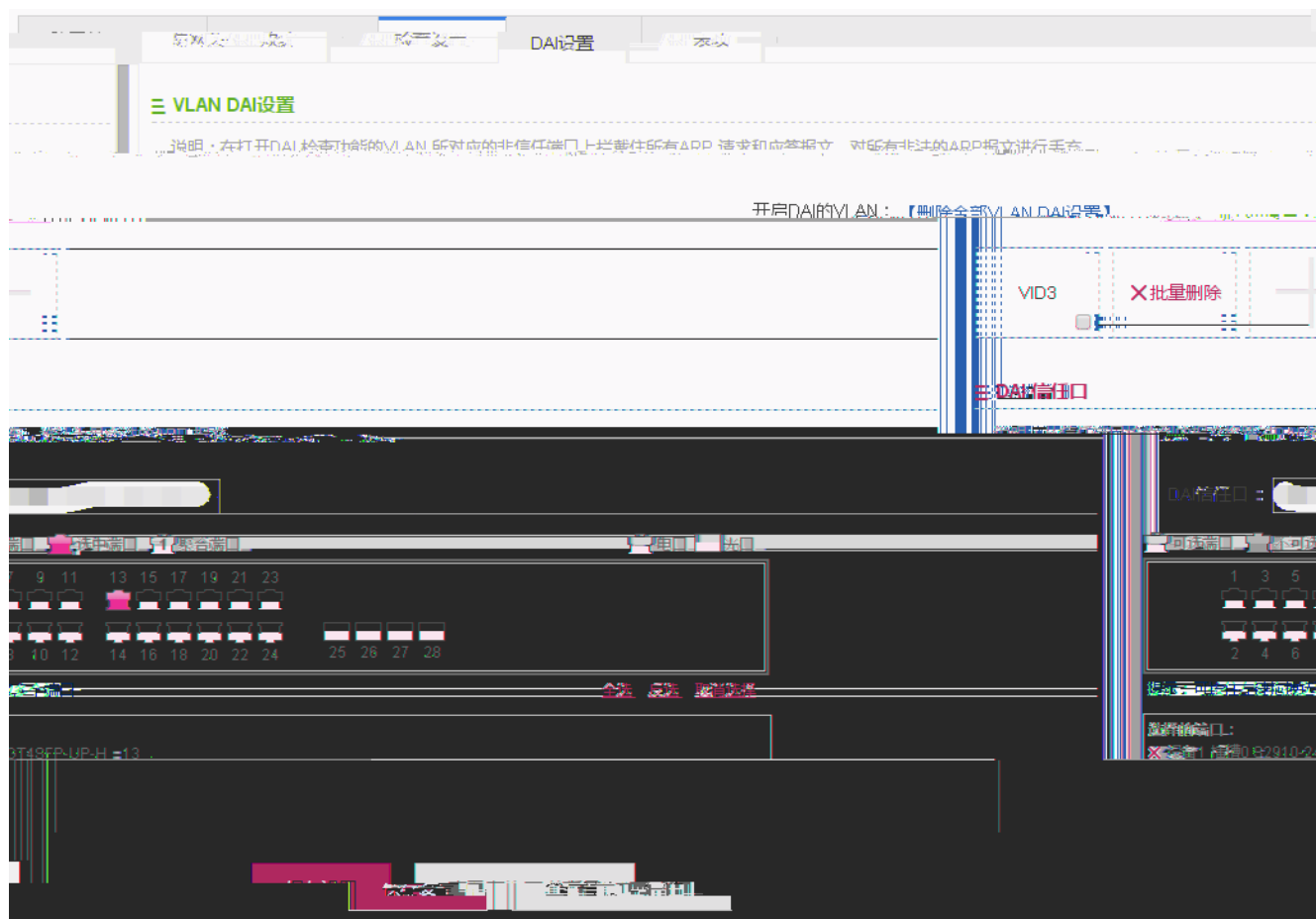
说明：对开启ARP检查功能端口下的所有的ARP报文进行过滤，对配置中的ARP报文进行丢弃，防止有恶意攻击者在网络中ARP欺骗，提高网络的稳定性。



ARP

  ARP  ARP

 DHCP Snooping ARP



1 VLAN DAI

DAI VLAN

2 DAI

DAI



DAI

防网关ARP欺骗 ARP检查设置 DAI设置 **ARP表项**

动态>>静态绑定 解除静态绑定 手工绑定 基于IP地址查询:

IP地址	MAC地址	类型	操作	IP地址
1414.4b72.fa9b	动态绑定	动态>>静态绑定	<input type="checkbox"/>	172.18.124.1
b8ac.6f40.50e8	动态绑定	静态>>动态绑定	<input type="checkbox"/>	172.18.124.17
b8ac.6f3e.fa9c	动态绑定	静态>>动态绑定	<input type="checkbox"/>	172.18.124.52
C8CB.2A10.C101	动态绑定	静态>>动态绑定	<input type="checkbox"/>	172.18.124.55

动态绑定 解除静态绑定 手工绑定 动态>>静态绑定 静态>>动态绑定 动态>>静态绑定

显示: 10/10 条, 共 8 条

>>

1 ARP

2 ARP < >

1 ARP

2 ARP < >

IP MAC

ARP

1.3.4.3 IP Source Guard

IP Source Guard

1-29

接口配置 用户绑定

说明：IP Source Guard可以防止用户伪造IP地址及防止用户变化源IP的拒绝行为，要求用户必须动态DHCP方式获取IP，否则将无法连接网络。

+ 添加开启IP Source Guard端口 × 删除选中的IP Source Guard端口

操作	IP地址	MAC地址	端口	IP Source Guard
IP-ONLY			Active	Deny-All
				删除

删除 G11/0/5

显示: 10 条 共1条

	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	<	>	

1-30

接口配置 用户绑定

说明：当开启IP Source Guard的功能的端口会过滤所有非DHCP的IP报文,配置用户绑定的静态地址后，端口允许静态绑定的IP报文通过。

+ 添加绑定 × 删除选中的绑定

	MAC地址	IP地址	VLAN ID	端口	操作
无记录信息					

显示: 10 条 共0条

1 确定

MAC IP VLAN ID

< > <

>

1

2

< > ?

1.3.4.4

1-31

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					

显示: 条 共0条

IP

< > <

>

1

2

< >

?

1-32

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 1 确定

IP

< > <

1

2

< >

1.3.4.5 NFPP

NFPP

1-33 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扫描防攻击： 开启IP扫描防攻击，防止大量非法IP扫描报文攻击设备。设备每秒处理的IP扫描报文 **不超过4个**。
[【IP扫描列表】](#)

ICMP防攻击： 开启ICMP防攻击，防止大量非法ICMP报文攻击设备。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池被恶意请求耗尽地址池，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池被恶意请求耗尽地址池，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】](#)

1.3.4.6

风暴控制

+ 添加风暴控制端口 - 删除选中的风暴控制端口

未知名单播	操作	端口	广播	组播
-	编辑 删除	<input type="checkbox"/> Gi1/0/1	-	-
70%	编辑 删除	<input type="checkbox"/> Gi1/0/2	50%	60%
-	编辑 删除	<input type="checkbox"/> Gi1/0/3	-	-
5	编辑 删除	<input type="checkbox"/>		Gi1/0/4
5	编辑 删除	<input type="checkbox"/>		Gi1/0/5
7	编辑 删除	<input type="checkbox"/>		Gi1/0/6
3	编辑 删除	<input type="checkbox"/>		Gi1/0/7
3	编辑 删除	<input type="checkbox"/>		Gi1/0/8
0	编辑 删除	<input type="checkbox"/>		Gi1/0/9

端口保护

说明：设为保护口的端口之间无法互相通讯。面板初始选中的端口为当前的保护口，可点击“显示当前保护口”刷新面板。

设置选中端口为保护口：

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				
2	4	6	8	10	12	14	16	18	20	22	24	25	26	27	28

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：

1.3.5.2 DHCP

DHCP

DHCP

DHCP

DHCP

1-36 DHCP

DHCP配置		静态地址分配	客户端列表
默认网关	租用时间	DNS	操作
40.40.0-1-40.40.255.254	40.40.255.254	20小时	编辑 删除
显示: 10 条 共1条		首页	

DHCP

IP

DHCP

DHCP

DHCP

< >

DHCP

< >

DHCP

1 DHCP

DHCP

2 DHCP

< >

DHCP

DHCP

<DHCP > DHCP

1-37

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							

10 条记录 | 首页 < 上一页 下一页 > 末页 | 1

IP MAC

< >

< >

1

2

< >

1-38

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 DHCP

DHCP

1-39 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发给客户端。

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

1.3.5.4 ACL

ACL

ACL

1-40ACL

The screenshot shows the Eweb ACL configuration interface. At the top, there are tabs for 'ACL列表', 'ACL时间', and '应用ACL'. Below the tabs, there are buttons for '删除ACL', '+添加ACE规则', and 'X删除选中'. On the right, there is a dropdown menu for 'ACL列表' with the value 'test' and a '添加ACL' button. The main area contains a table with the following columns: '访问控制', '协议', '目的IP/通配符', '目的端口', '生效时间', '状态', and '操作'. The table is currently empty, displaying '无记录信息'. At the bottom, there are navigation controls including '页', '页', '页', '页', '1', '条', '10', '条', '条', and '条'.

ACL
ACL ACL ACL ACL
ACL
ACL
ACL 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
-------	-------	-------

+ 添加时间对象 X 删除选中时间对象

<input type="checkbox"/>	时间对象	时间周期	时间段	操作
<input type="checkbox"/>	worktime	工作日	8:00-16:00	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

ACL

ACL

ACL

ACL

< >

ACL

<

>

ACL

ACL

ACL

ACL

1-42 ACL

ACL时间	应用ACL
-------	-------

应用端口 X 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

显示: 10 条共2条 << 首页 < 上一页 1 下一页 > 末页 >> 1 确定

ACL

ACL

ACL

ACL

ACL

ACL

< >

ACL

<

>

ACL

1 ACL

ACL

2 ACL

< >

1.3.5.5

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

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

1页 < 上一页 下一页 > 末页 1 确定

显示: 10 条 共0条

< >

< >

< >

1

2

< >

1-45

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				

1/1 条

首页 < 上一页 下一页 > 末页

1 确定

显示: 10 条

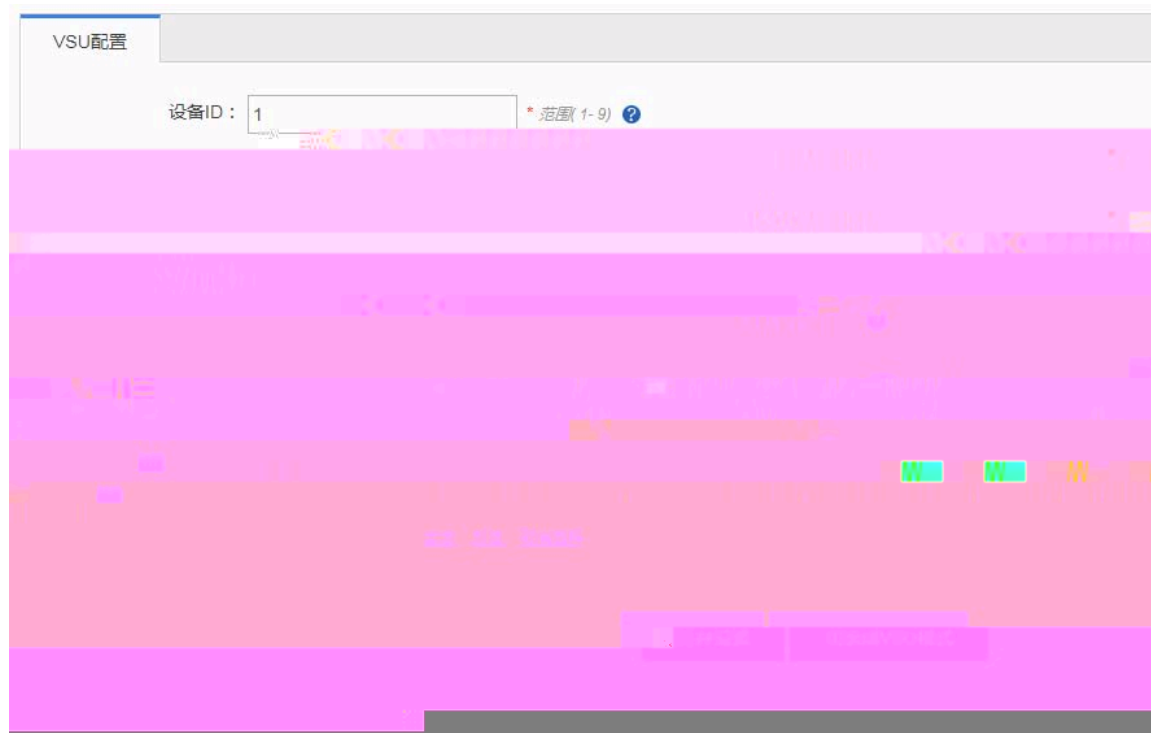
1 < >

2 < >

1.3.5.6 VSU

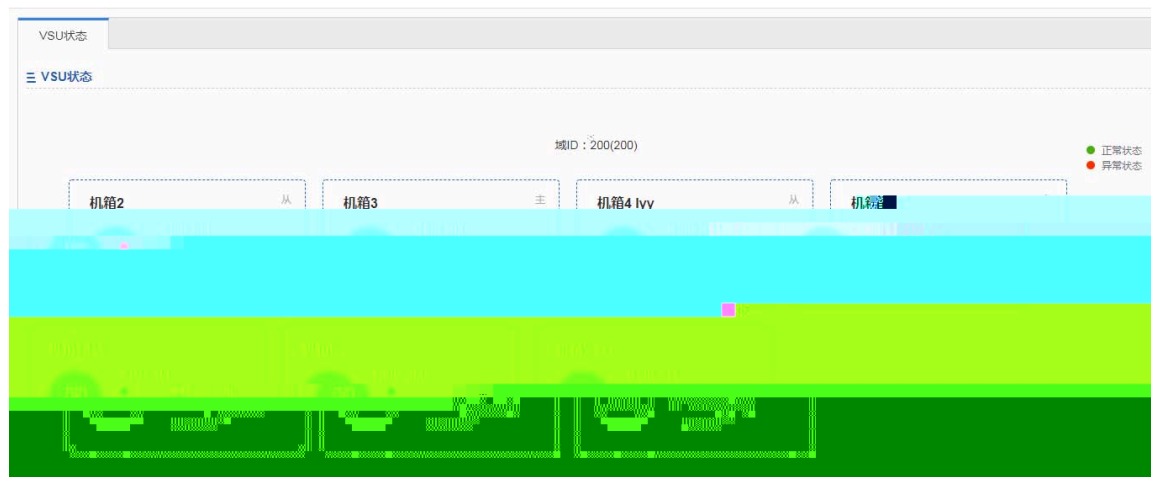
VSU

VSU



VSU

VSU



VSU



1.3.6

Web

1.3.6.1

SNMP

DNS

1-46

Internet

< >

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

≡ 导入/导出配置

说明：导入过程中不能关闭或者刷新页面，否则导入将失败！导入配置后，要启用新的配置，请在本页面重启设备否则配置不生效。

文件名：

≡ 恢复出厂设置

说明：恢复出厂设置，将删除当前所有配置。如果当前系统存在有用的配置，可先 [导出当前配置](#) 后再恢复出厂设置。

[【查看当前配置】](#)

/

< >

1-49

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：

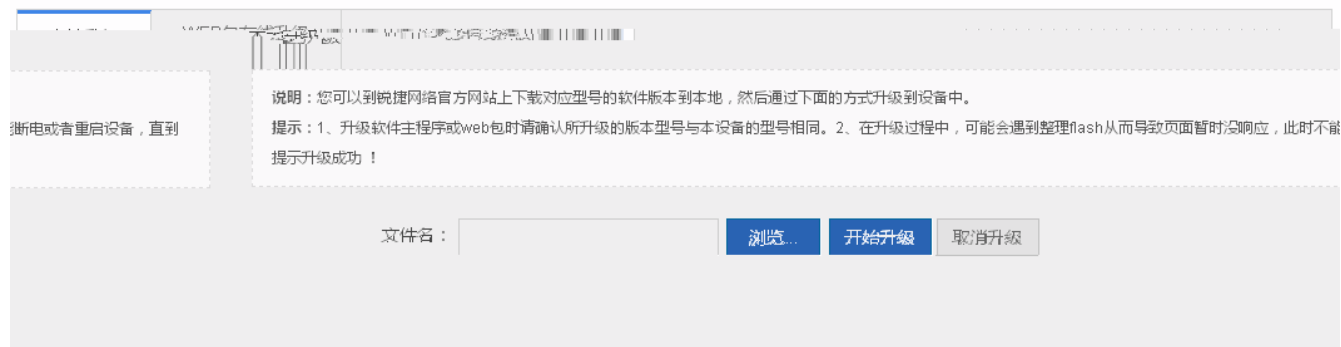
WEB

< >

1.3.6.2

WEB

1-52

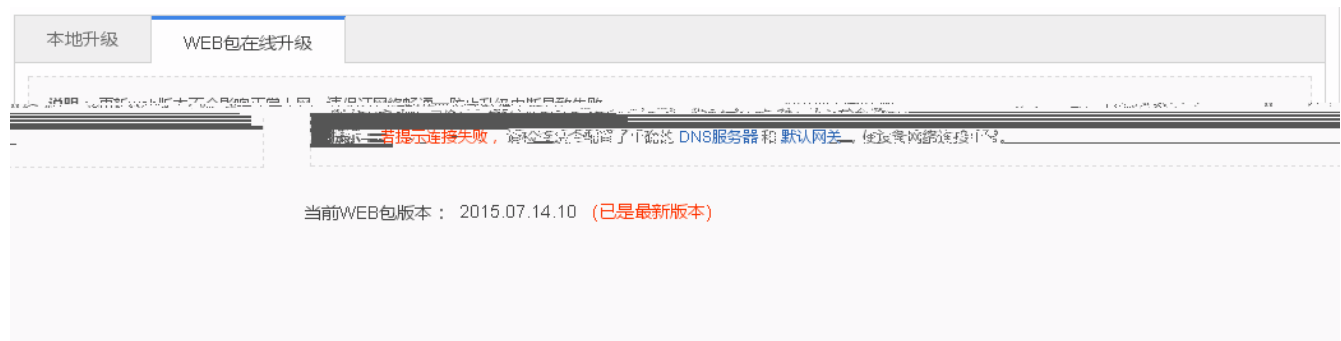


bin < >

WEB

WEB

1-53 WEB



< > WEB

1.3.6.3

ping检测 **tracert检测** 线缆检测

目的IP地址或域名 : *

超时时间(1-10) :

重复次数(1-100) :

IP

< >

tracert

tracert

1-58 tracert

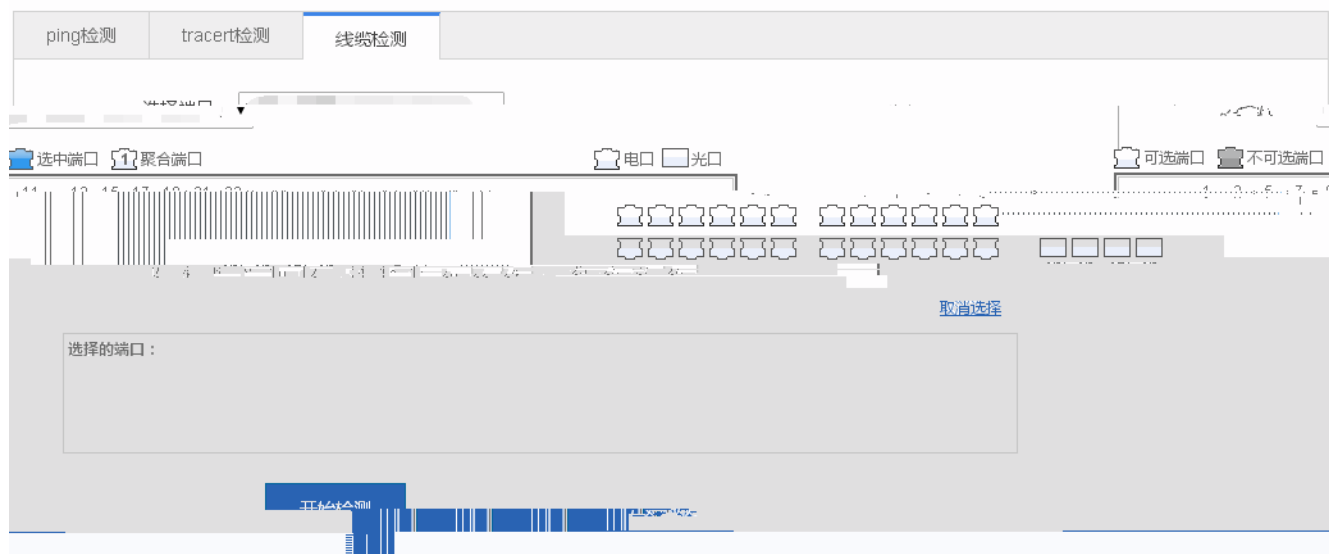
ping检测 **tracert检测** 线缆检测

目的IP地址或域名 : *

超时时间(1-10) :

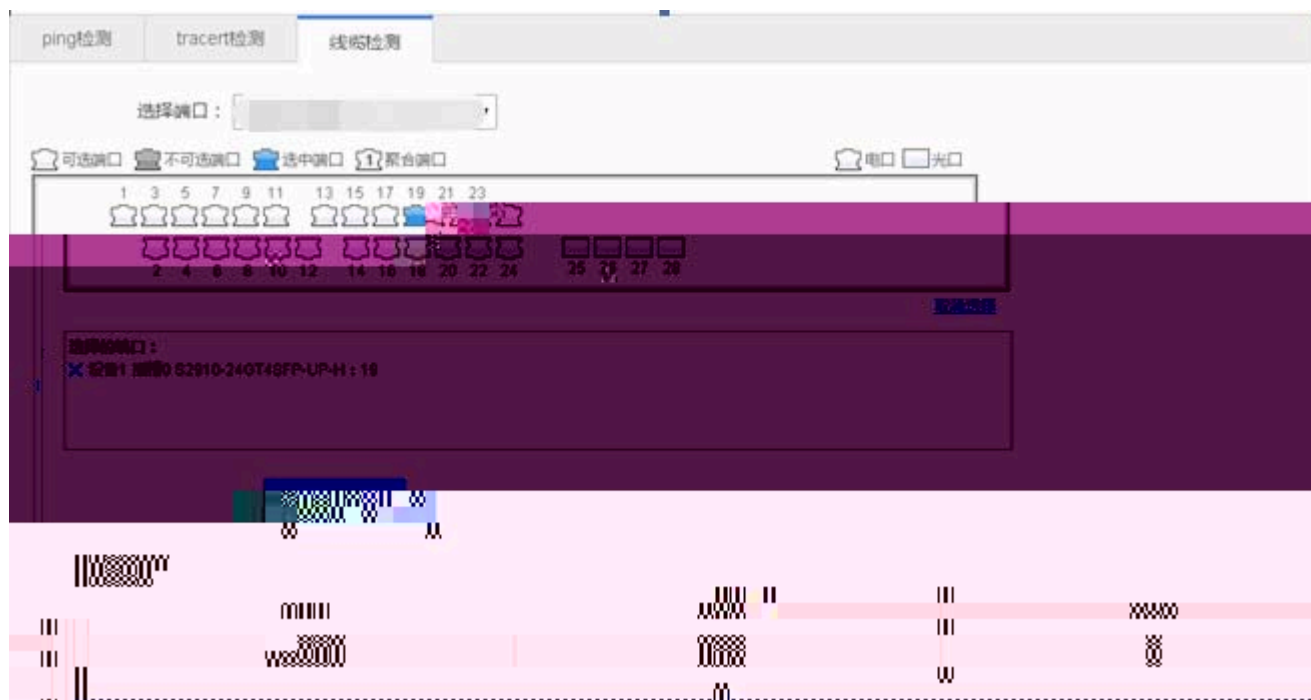
ping IP < >

1-59



< > < >

1-60



1.3.6.6 WEB

CLI

CLI

TAB

?

