

WEB—)5z »

RG-S2910 . 'çA E Ñ

S2910_RGOS11.4(1)B3 · {

" , yV1.0

IUV_MK0Z j 6 iHàl

copyright © 2016 i H àl

+ , C , Ò ¢ % † ä Ó o

ì - æ i H àl 0 μ U k ' ~ % y y K - Y ' ~ ¢ ¥ + , B ^a ~ ¢ ¶ B g Ò d Ì o Č ao
wo n no ì Ł ĺ U \$ o 1 ĺ ¶ B ¢ B ^a 9 (o



Y fi i H àl ð

, UC ĺ U æ ~ ö ¢ h ~ ö k _ æ ~ K (~ o

Ó æ ~ 1 D } o ~ ¢ Ò I ' c y Ú † Ø k , T ¶ B ¢ B ^a D } o ~ ¢ Ò U ¢ Ó ~
1 ¢ 8 \$ ~ o † ' c P ~ † k i H àl + , ~ ' ~ ¢ P ¢ ó P Ò ¢ ¢ o

9 D } ~ , · ¢ ĺ U = k , ~ k ° g % o i H àl ¢ Z ~ ' ~ * = ¢ æ U P Č Ñ + ~
g w Ó o

, ð ~ N 6 - o i H àl ¢ Ú , ð ~] @ ĺ ~ Č G U · k x w G ð ~ ¶ Z ~ j ¢ ¢ 4 ¥ k
, ð ~ æ ~ , - ^a Ł ' ~ ¢ P ¢ „ P o

0 ‘ çK t fl

àlWid

—PzKt

àl òt

iHàl à{y <http://www.ruijie.com.cn/>

iHàl ¢ ¸ ~y <http://webchat.ruijie.com.cn>

iHàl à{~ u4~†y <http://www.ruijie.com.cn/service.aspx>

7 24 4 —~ % ¸ y4008-111 -000

iHàl — ·y <http://bbs.ruijie.com.cn/portal.php>

o |°\«y <http://www.ruijie.com.cn/service/know.aspx>

iHàl —u4 FØ y4008111000@ruijie.com.cn

1.

xXg ¢#òy

y xXg ... p g xX 4 J • À`ÿ B^hJ }nPo

} y xXg @ g xX • À g`W B^hJ }nP

[] ynP [] , Ü B^k ¢ xXF â 'U# o

{x|y|...} ynPR Œ Ú # ¼ # H%† o

[x|y|...] ynPR Œ Ú # ¼ # H%† Œ æ #o

//y E Û ÷ gnP hKgo

2.

0 J __l) ö” ÛhP ¢ q i ¥ Ôh ¢ “ k ? ö” ¢#òy



/

3.

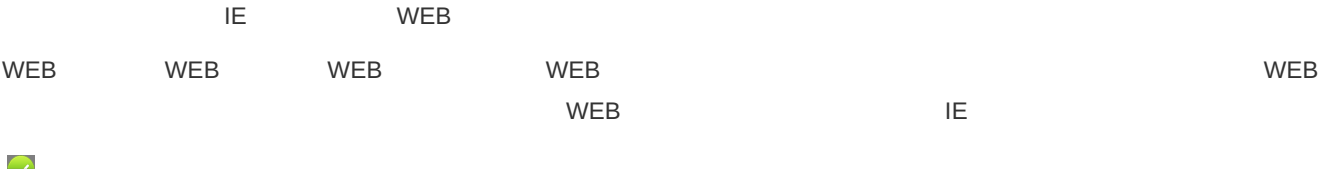
¸ô~ “¢Bª M "c U k q <}7`_D}æu4 M " gFå

¸ô~Bª “P ¸ U m~¿ D}'ç ~ gòD}"Zo T lkÀ}"P ¸<Y
Õ ¸ Õ

¸ô~ C Ł CŁ D}£ökWn4%†"▷# Ł kYC g4Ł # CAEÑ

1 Eweb

1.1



PC ping WEB

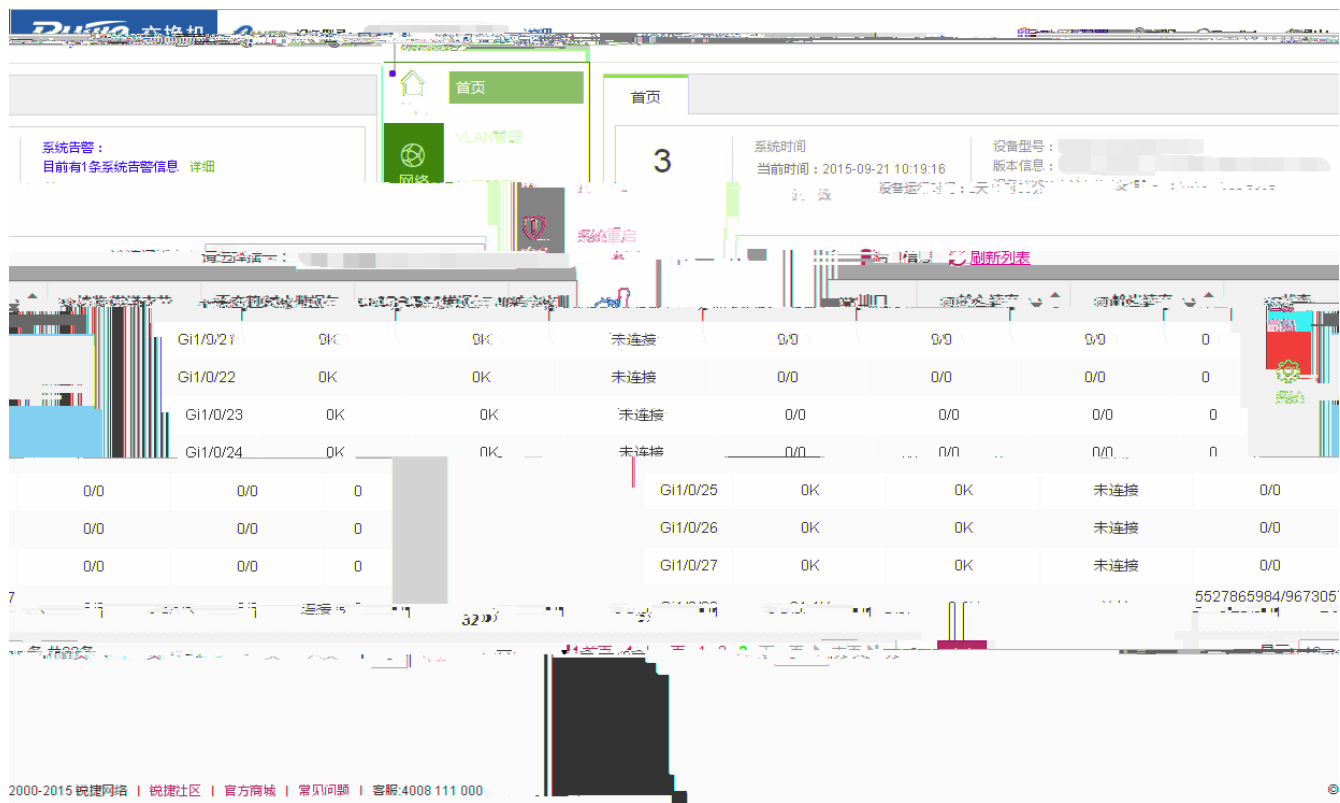
WEB WEB PC

360 IE7.0 IE8.0 IE9.0 IE10.0 IE11.0 Google chrome IE
WEB
1024*768 1280*1024 1440*960 1920*1080

 WEB "write" WEB
WEB

WEB

1-2 http://X.X.X.X IP



1.3 Eweb

/	
编辑	
删除	
ON	
1	

	Trunk	VLAN	/VLAN
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

 Trunk口

 电口

 光口

13 15 17 19 21 23



25 26 27 28



1 3 5 7 9 11



2 4 6 8 10 12



14 16 18 20 22 24



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：

选择的端口：

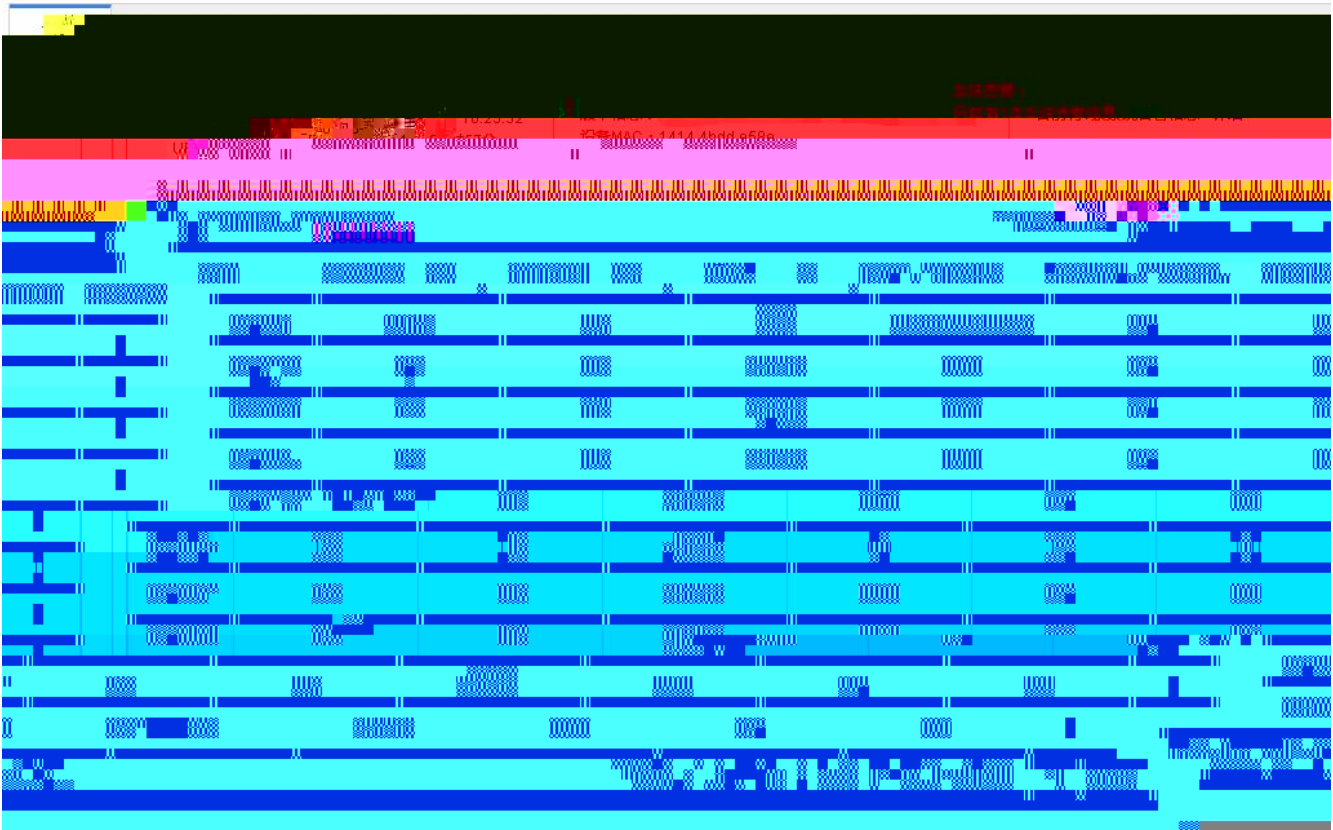
✘ 设备1 插槽0 S2910-24GT4SFP-UP-H : 3-4

VLAN	VLAN Trunk
MAC	
	RLDP
IGMP	IGMP Snooping
DHCP	DHCP

	ping tracert

1.3.2.1

1-5



1.3.2.2 VLAN

VLAN VLAN Trunk

VLAN

VLAN

1-6 VLAN

VLAN设置

Trunk口设置

+批量添加VLAN

+添加VLAN

✕删除选中VLAN

☐	VLAN ID	VLAN名称	IPv4 IP	掩码	端口	操作
☐	1	VLAN0001	172.18.124.73	255.255.255.0	Gi0/1-10, Gi0/13-16, Gi0/25-26 Ag2, Ag7, Ag25	编辑
☐	2	VLAN0002			Gi0/13-14	编辑 删除
☐	4	HHHHfffjh			Gi0/13-14	编辑 删除
☐	5	VLAN0005			Gi0/13-14	编辑 删除
		Gi0/13-14				删除
		Gi0/13-14				删除
		Gi0/13-14				删除
		Gi0/13-14				删除
255.255.255.0		Gi0/13-14				删除
		Gi0/13-14				删除

显示 10 条 共 14 条

☐	6	VLAN0006				
☐	7	VLAN0007				
☐	14	VLAN0014				
☐	15	VLAN0015				
☐	16	6fffffffffffffffff	12.36.36.65			
☐	17	VLAN0017				

VLAN

VLAN VLAN ID VLAN

VLAN

VLAN < > VLAN < >

VLAN

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：源MAC与目的MAC

保存设置

恢复默认值

三 聚合口设置

[illegible]

1-10

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到转发给目的端口的端口上, 源端口上流量激增, 会极大影响源端口的转发性能, 所以建议将源端口设置为聚合端口。

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

1 聚合端口

电口

光口

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

选择的端口:
✖ 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)

1 3 5 7 9 11 13 15 17 19 21 23

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

取消 全选

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

配置规则

设备1 插槽0 S2910-24GT4SFP-UP-H : 13

设备1 插槽0 S2910-24GT4SFP-UP-H : 13

web

<

>



<

>



1-13

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

☐	MAC地址	VLAN ID	操作
☐	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

1-15

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 的优先级来的高。

+ 添加静态路由

+ 添加默认路由

✕ 删除选中路由

☐	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

生成树全局设置

生成树端口设置

RLDP设置

三 全局设置

生成树开关：

ON

优先级：

8

范围(0-15)，默认8

握手时间：

2

范围(1-10)秒，默认2

老化时间：

300

范围(10-1800)秒，默认300

转发延迟：

1000

范围(1-1800)秒，默认1000

生成树模式：

MSTP

保存设置

三 MST 设置

+ 添加实例

× 删除选中实例

操作	实例值	VLAN	优先级
默认实例，不可编辑	0	ALL	8

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

+ 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	直拉基型	生成树	操作
关闭	关闭	关闭	关闭	point-to-point	0/0/128	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	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	关闭	关闭

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

显示 10 条 共48条

Port Fast BPDU

< >

< >

RLDP

The diagram illustrates the evolution of a network structure. At step 1, there are two nodes, each labeled 'RLDP'. At step 2, the network has grown to include more nodes and connections, with 'RLDP' labels still present on some nodes. The diagram shows a progression from a simple two-node structure to a more complex, interconnected network.

1.3.3.4 IGMP

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

三 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

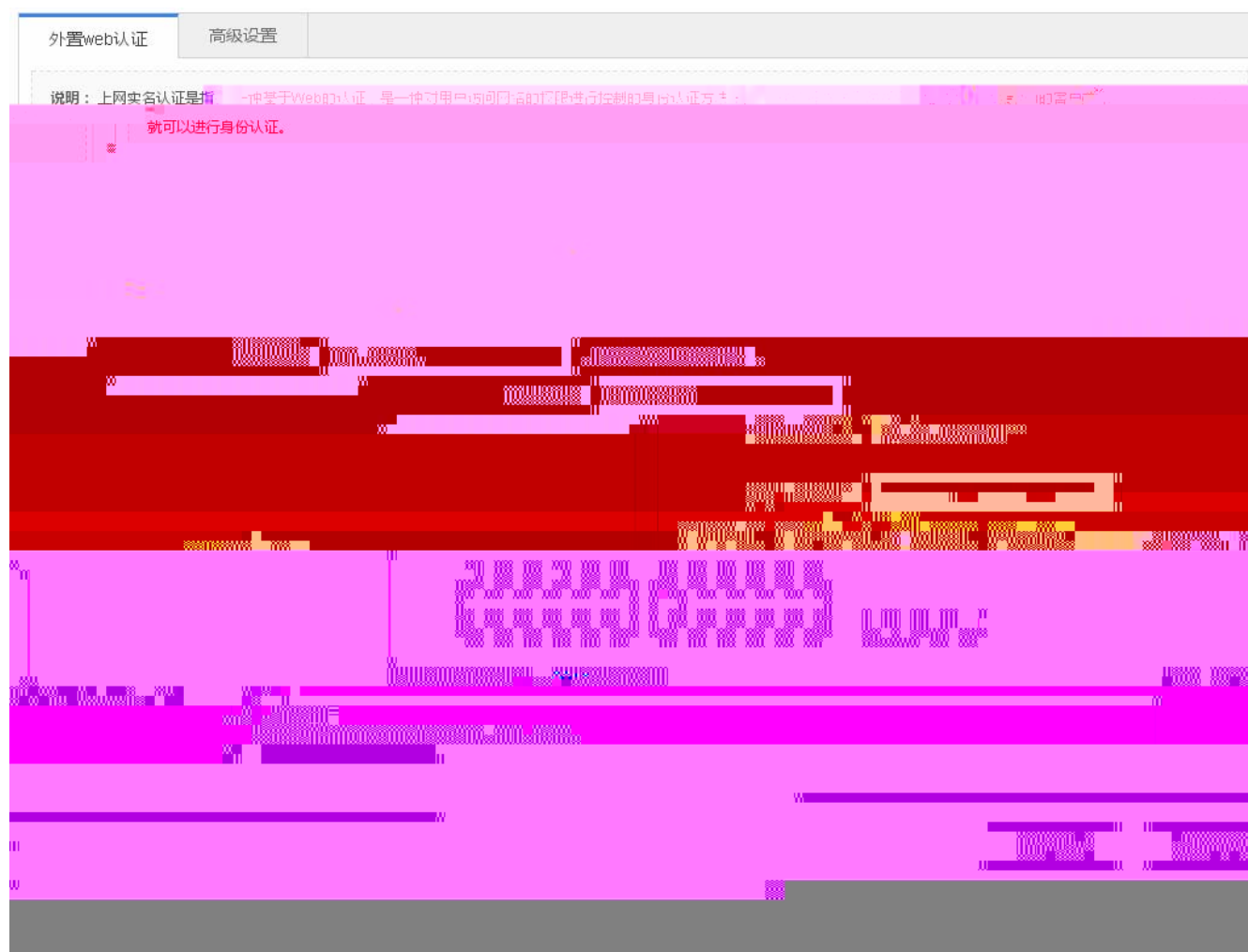
web

web

web

1-20

web



IP

1-21

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

☐	过滤端口	IP	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

< >

< >

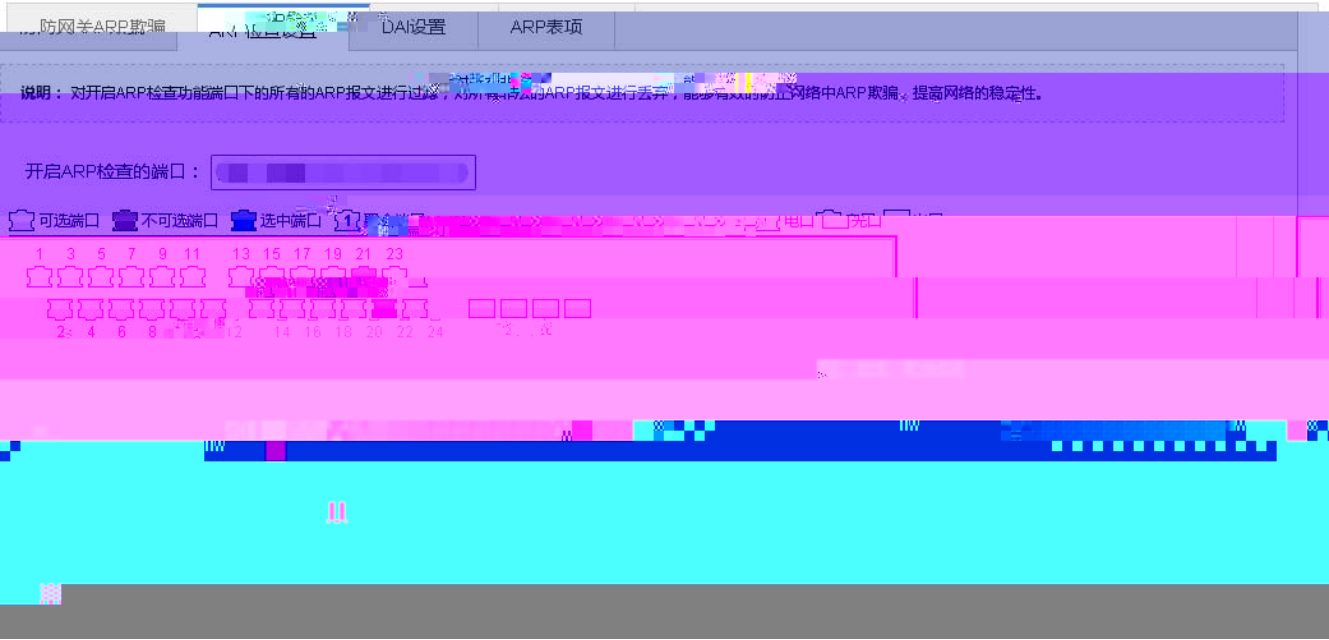
1

2

< >

ARP

1-24 ARP



ARP



< ARP > ARP

 DHCP Snooping ARP

DAI

1-25 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：

搜索

	IP地址	MAC地址	类型	操作	
静态绑定	☐	172.18.124.1	1414.4b72.fa9b	动态绑定	动态>>
静态绑定	☐	172.18.124.17	b8ac.6f40.50e8	动态绑定	动态>>
静态绑定	☐	172.18.124.52	b8ac.6f3e.fa9c	动态绑定	动态>>
静态绑定	☐	172.18.124.55	0000.0000.0000	动态绑定	动态>>

静态绑定

动态>>静态绑定

解除静态绑定

手工绑定

1

确定

显示 10 条 共 8 条

>>

1 ARP

2 ARP < >

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

IP-ONLY	Active	Deny-All	删除	G1/0/5

◀ 首页

◀ 上一页

1

下一页 ▶

末页 ▶

1

确定

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

< >

1-28

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

◀ 首页

◀ 上一页

下一页 ▶

末页 ▶

1

确定

MAC IP VLAN ID

< > <

>

1

2 < > ?

1.3.4.4

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，设备每秒处理报文 不超过15个。

查看防攻击日志：[【本地防攻击日志】](#)

保存设置 恢复默认设置

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

-

编辑

删除

70%

编辑

删除

-

编辑

删除

端口

广播

组播

Gi1/0/1

-

-

Gi1/0/2

50%

60%

Gi1/0/3

-

-

删除

17 / 18

5

-

-

-

删除

Gi1/0/4

6

-

-

-

删除

Gi1/0/5

7

-

-

-

删除

Gi1/0/6

8

-

-

-

删除

Gi1/0/7

9

-

-

-

删除

Gi1/0/8

10

-

-

-

删除

Gi1/0/9

11

-

-

-

删除

Gi1/0/10

< >

<

>

1

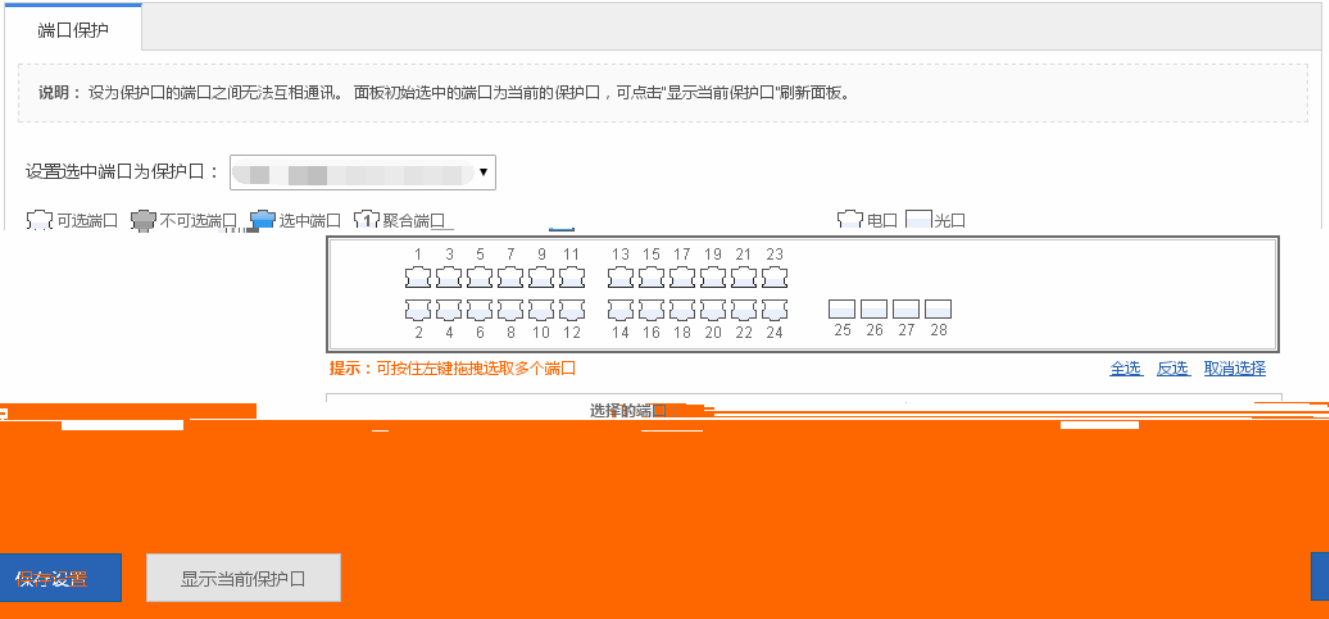
2

< >

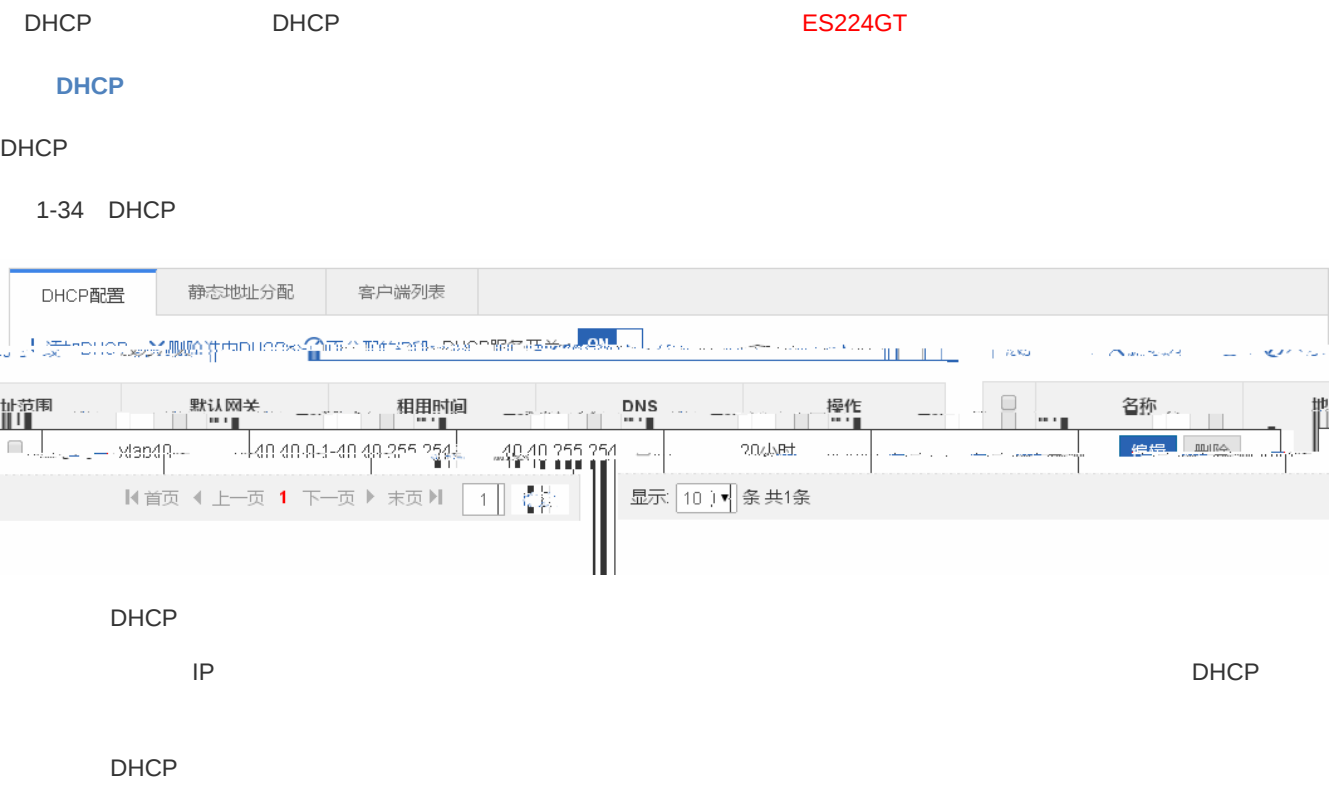
1.3.5

1.3.5.1

1-33



1.3.5.2 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

✕ 删除选中地址

☐	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

< >

1-36

DHCP配置

静态地址分配

客户端列表

把MAC地址绑定到静态获取的IP上

删除选中客户端

手工IP地址查询

确定

☐	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

ACL

ACL < > ACL <

>

ACL

1 ACL

2 ACL < >

ACL

ACL

ACL

ACL

1-38 ACL

ACL列表

ACL时间

应用ACL

+添加时间对象

✕删除选中时间对象

☐	时间对象	时间周期	时间段	操作	
☐	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 <

>

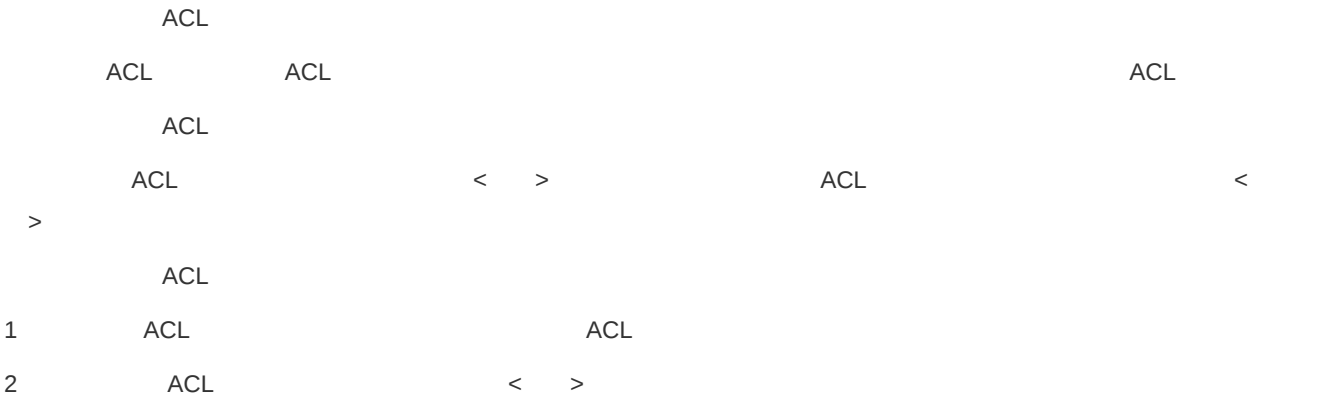
ACL

ACL

ACL

ACL

1-39 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

✕ 删除选中的分类

	分类名	ACL	操作
☐	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

× 删除选中规则

操作	类名	带宽(Kbps)	突发流量(KBytes)	带宽超出处理
无记录信息				

一页 ▶ 末页 ▶▶

1

确定

显示: 10

条 共0条

◀ 首页 ◀ 上一页 下

< >

< >

< >

1

2

< >



Internet

< >

1-44

WEB

< >

SNMP

SNMP

1-47 SNMP

系统时间

修改密码

恢复出厂设置

增强功能

SNMP

DNS

SNMP版本：☐ v2版本 ☒ v3版本

设备位置：

SNMP口令：

加密密码：

认证密码：

Trap口令：

Trap社区名：

保存设置

清除设置

SNMP

SNMP

Trap

< >

DNS

DNS

1-48 DNS

系统时间

修改密码

恢复出厂设置

增强功能

SNMP

DNS

DNS服务器1：

保存设置

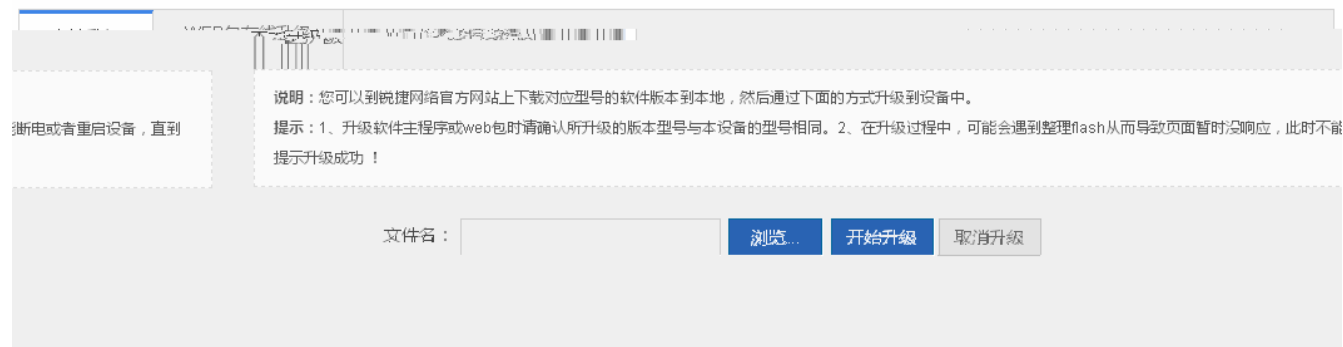
DNS

< >

1.3.6.2

WEB

1-49



bin

<

>

WEB

WEB

1-50 WEB



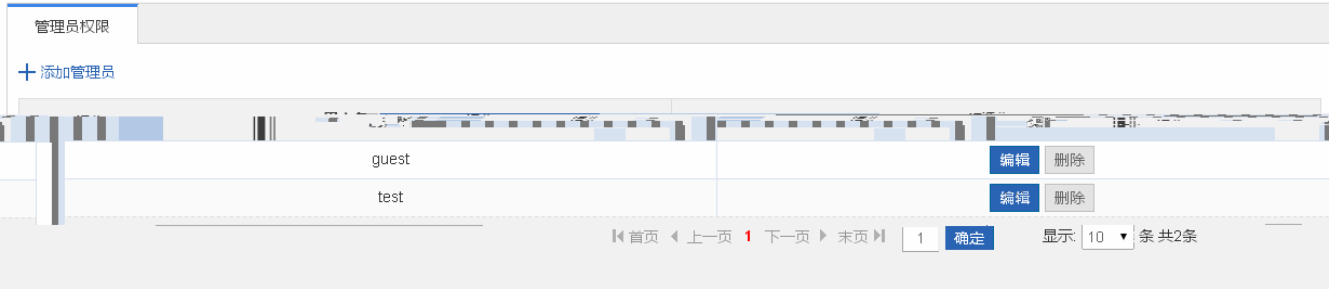
<

>

WEB

1.3.6.3

1-51



< >



admin

“ ”

1.3.6.4

1-52



IP

SYSLOG

1-53

更新当前系统版本

$$L = 1.29 \times 10^{-2} \text{ m} \quad \Rightarrow \quad \lambda = \frac{2L}{n} = \frac{2(1.29 \times 10^{-2} \text{ m})}{2} = 1.29 \times 10^{-2} \text{ m}$$
[illegible]

Console logging: level debugging, 659 messages logged

Buffer logging: level debugging, 659 messages logged

Timestamp debug messages: datetime

Timestamp log messages: datetime

Sequence-number log messages: disable

Counting misspelled words

Log Buffer (Total 131072 Bytes): 32566-written, 47225

*Jan 1 08:00:34: %LOCAL_DP-5-LC_FROE: Board information in this chassis has been col

*Jan 1 08:00:34: %SWITCH-6-INSTALL: Install chassis ES224 on switch 1

lected.

Figure 1. The effect of the concentration of the *Agrobacterium* suspension on the transformation efficiency of *Agrobacterium* strains.

[illegible]

2010年12月31日

Each 1000000% (1000000% (1000000%)) POWER ON The power-on, used in single (with the (with the) power-on

Jan 1 LU46: %DP: 6-PROB: Board probing has completed.

ping tracet

ping

tracert

Ping

1-54 ping

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) : 开始检测		

IP

<

>

tracert

tracert

1-55 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) : 开始检测		

ping

IP

<

>