



—— 制造最可靠的网络设备 —— **UK5604 系列万兆交换机通用 WEB 配置手册**

# 优肯 UK5604 系列万兆交换机

## 通用 WEB 配置手册 V1.0.1

©copyright by Shenzhen Speed Technology Co.,Ltd. All rights reserved.

**声明：**事先未征得深圳市时速科技有限公司（简称：时速科技）的书面同意，任何人不得以任何方式拷贝或复制本文档中的任何内容。

### 深圳市时速科技有限公司

公司地址：深圳市龙华新区梅龙路与建设东路交汇处百富汇科技园 B 栋二楼

服务热线：400-6013-660

优肯官网：<http://www.speednt.com>

邮编：518109

编写人/修订人	审核人	版本	日期
NA	NA	V1.0.1	2013-12-18
-	-	-	-

### 注意事项：

此软件版本在配置功能完成后；除堆叠功能外；其它功能必须进入系统维护-配置保存-点击配置保存；否则重启设备后所有配置不保存。

**UK5604-52TC 万兆以太网交换机**

设备配置 | 设备状态 | 系统诊断 | 系统维护

- 重新启动设备
- 出厂默认值
- 软件上传
- 配置保存
- 配置下载
- 配置上传
- 配置激活
- 配置删除

保存当前配置到启动配置

请注意：生成该配置文件需要耗费时间的，具体时间取决于配置变化多少。

## 目 录

一、概述.....	3
二、设备配置.....	3
1、信息.....	3
2、IP 配置.....	4
3、NTP 配置.....	4
4、Time.....	4
5、日志.....	5
6、用户管理配置.....	5
7、访问管理.....	6
8、SNMP.....	6
9、端口配置.....	7
10、端口安全.....	8
11、端口隔离.....	8
12、ACL.....	8
13、聚合.....	14
14、环路保护.....	16
15、生成树.....	16
16、ARP 检查.....	19
17、DHCP 探测配置.....	21
18、IGMP 监听.....	22
19、MAC 地址表.....	23
20、VLANS 配置.....	24
21、镜像.....	27
22、堆叠.....	27
三、设备状态.....	28
1、系统.....	28
2、端口.....	29
3、网络安全.....	30
四、系统诊断.....	36
1、PING.....	36
2、VeriPHY.....	37
五、系统维护.....	37
1、重新启动设备.....	37
2、出厂默认值.....	37
3、软件上传.....	38
4、配置保存.....	38
5、配置下载.....	38
6、配置上传.....	39
7、配置激活.....	39
8、配置删除.....	40
六、硬恢复出厂设置.....	40

## 一、概述

为了便于客户更好的使用本公司的产品；该指导手册描述了在 Web 上配置 UK5604 交换机功能的基本方法。

如果想通过web访问交换机，需要确保您的计算机已经连接到交换机所在的网络；如果是第一次使用交换机，无需对交换机做额外配置，您就可以使用Web 访问。**按如下操作即可：**

- 1、修改您计算机网络适配器的 IP 地址为“192.168.0.2”，子网掩码为“255.255.255.0”
- 2、打开Web 浏览器，在地址栏中输入“192.168.0.10”。其中“192.168.0.10”是交换机的缺省管理地址。
- 3、在登录验证对话框中输入用户名和密码，初始的用户名和密码均为“admin”，请注意区分字母的大小写。
- 4、若认证成功，浏览器中会显示交换机的系统设备端口信息页。如下图所示：



说明：

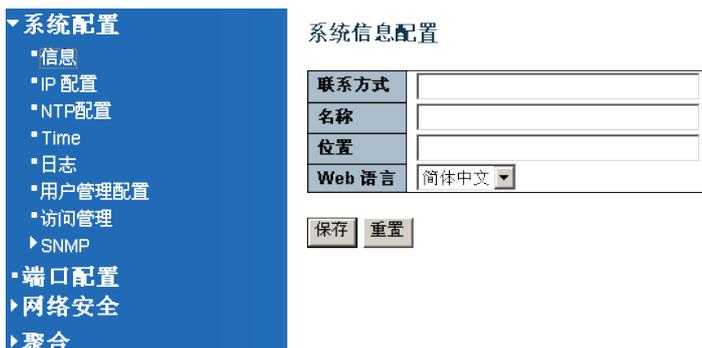
1. 绿色指示灯表示设备工作正常
2. 端口 3 表示 link 处于 UP 状态，其它端口都为 DOWN
3. 页面左侧部分为配置导航栏；主要分为四大块：设备配置、设备状态、系统诊断、系统维护；

## 二、设备配置

这部分是设备的所有功能的配置，其中包括了系统配置、端口配置、安全、聚合、环路保护、生成树、组播、链路发现协议、MAC、VLAN、私有 vlan、QoS、镜像、堆叠配置；

### 1、信息

配置 Web 语言中英文切换，联系方式、名称、位置：



## 2、IP 配置

此页面修改本设备 WEB 的 IP 地址配置：

▼ 系统配置

- 信息
- IP 配置
- NTP配置
- Time
- 日志
- 用户管理配置
- 访问管理
- ▶ SNMP
- 端口配置

### IP 配置

删除	VLAN	IPv4	
		地址	掩码长度
<input type="checkbox"/>	1	192.168.0.10	24

## 3、NTP 配置

NTP 时间同步功能，只需要配置对应 NTP 服务器地址即可；模式开启 如下图：

▼ 系统配置

- 信息
- IP 配置
- NTP配置
- Time
- 日志
- 用户管理配置
- 访问管理
- ▶ SNMP
- 端口配置
- ▶ 网络安全

### NTP配置

模式	开启
服务器1	192.168.0.151
服务器2	
服务器3	
服务器4	
服务器5	

## 4、Time

时区配置默认为下图设置即可，结合 NTP 配置使用：

▼ 系统配置

- 信息
- IP 配置
- NTP配置
- Time
- 日志
- 用户管理配置
- 访问管理
- ▶ SNMP
- 端口配置
- ▶ 网络安全
- ▶ 聚合
- 环路保护
- ▶ 生成树
- ▶ IP Source Guard
- ▶ ARP 检查
- DHCP探测配置
- ▶ IGMP监听
- MAC 地址表
- VLANs配置
- 镜像
- 堆叠

### 时区配置

Time Zone Configuration	
时区	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
术语	China (0 - 16 字符)

### 夏令时配置

夏令时模式	
夏令时	关闭

起始时间	
月	1月
日期	1
年	2000
时	0
分	0
结束时间	
月	1月
日期	1
年	2000
时	0
分	0
偏移配置	
偏移	1 (1 - 1440) 分

## 5、日志

此页面配置系统日志配置：

▼ 系统配置

- 信息
- IP 配置
- NTP配置
- Time
- 日志
- 用户管理配置
- 访问管理
- ▶ SNMP
- 端口配置

### 系统日志配置

<b>服务器设置</b>	开启 ▼
<b>服务器地址</b>	<input type="text"/>
<b>系统日志级别</b>	信息 ▼

## 6、用户管理配置

此页面可以修 WEB 页面的管理用户密码；点击 admin 或添加新用户来添加或修改用户密码：

▼ 系统配置

- 信息
- IP 配置
- NTP配置
- Time
- 日志
- 用户管理配置
- 访问管理
- ▶ SNMP
- 端口配置
- ▶ 网络安全
- ▶ 聚合

### 用户配置

用户名字	特权级别
admin	15

▼ 系统配置

- 信息
- IP 配置
- NTP配置
- Time
- 日志
- 用户管理配置
- 访问管理
- ▶ SNMP
- 端口配置
- ▶ 网络安全

### 编辑用户

用户设置	
用户名字	<input type="text" value="admin"/>
密码	<input type="password"/>
密码(再次输入)	<input type="password"/>
特权级别	15 ▼

## 7、访问管理

此页面配置进入设备的 IP 段以及权限：

▼ 系统配置

- 信息
- IP 配置
- NTP配置
- Time
- 日志
- 用户管理配置
- 访问管理
  - ▶ SNMP
- 端口配置
- ▶ 网络安全
- ▶ 聚合

### 管理配置

模式

删除	VLAN ID	起始IP地址	结束IP地址	HTTP/HTTPS	SNMP	TELNET/SSH
添加新条目						

保存 重置

## 8、SNMP

简单网络管理协议配置, 系统默认开启:

▼ 系统配置

- 信息
- IP 配置
- NTP配置
- Time
- 日志
- 用户管理配置
- 访问管理
  - ▼ SNMP
    - 系统
    - Trap
    - Communities
    - 用户
    - 组
    - Views
    - 访问
- 端口配置
- ▶ 网络安全
- ▶ 聚合
- 环路保护
- ▶ 生成树
- ▶ IP Source Guard
- ▶ ARP 检查
- DHCP探测配置

### SNMP 系统配置

模式	开启
版本	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e50171000001

### SNMP 上报配置

抑制模式	关闭
抑制版本	SNMP v1
Trap Community	public
抑制目标地址	
抑制目的IPv6地址	::
抑制认证失败	开启
抑制连接与断开	开启
抑制报告模式	开启
抑制起时 (秒)	1
抑制重试次数	5

## 9、端口配置

可查看每个端口的连接状态,其中 1-24 或 1-48 号端口为设备前面板千兆端口,同时 21-24 或 45-48 号端口为复用端口,25-28 或 49-52 号端口为设备后面板万兆端口。

“链路” 状态指示红灯表示链路状态 down; 绿色表示链路状态 up。

端口速率模式: 若连接光纤, 则默认为“1000M 全双工”; 若连接网线, 则可选择“10M 半双工”、“10M 全双工”、“100M 半双工”、“100M 全双工”、“1G 全双工”、“自动协商”几种模式; 万兆端口: 可选择“10G 全双工”、“关闭”模式, 根据不同的线缆类型(电缆/光纤), 可选择相应的接入类型, 或“自适应”。

“电口”可开启端口流控开关, 实现端口流控。

“最大帧大小”, 可配置端口传输最大单元, 范围在 1522-10056 字节之间, 默认为 1522。

“冲突模式”, 当端口检测到冲突以后, 可选择“丢弃数据包”或“重启端口”。

“省电功能”, 可配置各种省电模式: 断开省电、连接省电、随时省电及关闭省电功能。

- ▶ 系统配置
- ▶ 端口配置
- ▶ 网络安全
- ▶ 聚合
- ▶ 环路保护
- ▶ 生成树
- ▶ IP Source Guard
- ▶ ARP 检查
- ▶ DHCP 探测配置
- ▶ IGMP 监听
- ▶ MAC 地址表
- ▶ VLANs 配置
- ▶ 镜像
- ▶ 堆叠

端口配置 for Switch 1

端口	链路	状态	速率	流控			最大帧大小	冲突模式
			模式	接收	发送	模式		
*			<>			<input type="checkbox"/>	1522	<>
1	●	未连接	自适应	×	×	<input type="checkbox"/>	1522	丢弃
2	●	未连接	自适应	×	×	<input type="checkbox"/>	1522	丢弃
3	●	1G双工	自适应	×	×	<input type="checkbox"/>	1522	丢弃
4	●	未连接	自适应	×	×	<input type="checkbox"/>	1522	丢弃
5	●	未连接	自适应	×	×	<input type="checkbox"/>	1522	丢弃
6	●	未连接	自适应	×	×	<input type="checkbox"/>	1522	丢弃
7	●	未连接	自适应	×	×	<input type="checkbox"/>	1522	丢弃
8	●	未连接	自适应	×	×	<input type="checkbox"/>	1522	丢弃
9	●	未连接	自适应	×	×	<input type="checkbox"/>	1522	丢弃
10	●	未连接	自适应	×	×	<input type="checkbox"/>	1522	丢弃
11	●	未连接	自适应	×	×	<input type="checkbox"/>	1522	丢弃
12	●	未连接	自适应	×	×	<input type="checkbox"/>	1522	丢弃
13	●	未连接	自适应	×	×	<input type="checkbox"/>	1522	丢弃
14	●	未连接	自适应	×	×	<input type="checkbox"/>	1522	丢弃
15	●	未连接	自适应	×	×	<input type="checkbox"/>	1522	丢弃
16	●	未连接	自适应	×	×	<input type="checkbox"/>	1522	丢弃
17	●	未连接	自适应	×	×	<input type="checkbox"/>	1522	丢弃
18	●	未连接	自适应	×	×	<input type="checkbox"/>	1522	丢弃

## 10、端口安全

此页面配置限制端口学习的 mac 个数，当学习的 mac 大于配置的时候会做相应的动作：

- ▶ 系统配置
- ▶ 端口配置
- ▶ 网络安全
  - 端口安全
  - 端口隔离
- ▶ ACL
- ▶ 聚合
- 环路保护
- ▶ 生成树
- ▶ IP Source Guard
- ▶ ARP 检查
- DHCP 探测配置

### 端口安全限制控制配置

系统配置

模式	关闭
超时使能	<input type="checkbox"/>
老化期	3600 秒

端口配置 for Switch 1

端口	模式	限制	处理模式	状态	重新开启
*	<>	4	<>		
1	关闭	4	无	关闭	重新开启
2	关闭	4	无	关闭	重新开启

## 11、端口隔离

显示端口隔离配置界面，此页面用来配置端口隔离，达到端口保护的效果。

例：假如 1 口连路由器，所有端口隔离，请参照下图：

- ▶ 系统配置
- ▶ 端口配置
- ▶ 网络安全
  - 端口安全
  - 端口隔离
- ▶ ACL
- ▶ 聚合
- 环路保护
- ▶ 生成树
- ▶ IP Source Guard
- ▶ ARP 检查
- DHCP 探测配置
- ▶ IGMP 监听
- MAC 地址表

### 端口隔离配置 for Switch 1

端口号																				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
<input type="checkbox"/>	<input checked="" type="checkbox"/>																			

## 12、ACL

### 1)、端口配置：

Policy ID: 选择某种策略应用到端口，配置范围[0-255], 默认为 0

处理模式: 转发是被允许还是拒绝，默认允许转发；

速率限制 ID: 端口上进行限速功能，ID 可配置 1-16，默认关闭，

端口重定向: 处理模式非允许下可以设置，默认关闭

LOG: 是否将端口接收帧保存到系统 log，默认关闭

Shutdown: 如果开启该功能那么从端口收到一个帧, 将会 disable 掉该端口, 默认关闭

状态: 重新开启该端口。默认开启

帧数量: 统计匹配该 ACE 的报文个数:

- 系统配置
- 端口配置
- ▾ 网络安全
  - 端口安全
  - 端口隔离
  - ▾ ACL
    - 端口
    - 速率限制
    - 访问控制列表
- 聚合
- 环路保护
- 生成树
- IP Source Guard
- ARP 检查
- DHCP 探测配置
- IGMP 监听

ACL端口配置for Switch 1

端口	Policy ID	处理模式	速率限制 ID	Port Redirect	记录Log	关闭端口	状态	帧数量
*	0	<>	<>	<>	<>	<>	<>	*
1	0	允许	关闭	关闭	关闭	关闭	开启	0
2	0	允许	关闭	关闭	关闭	关闭	开启	0
3	0	允许	关闭	关闭	关闭	关闭	开启	19830
4	0	允许	关闭	关闭	关闭	关闭	开启	0
5	0	允许	关闭	关闭	关闭	关闭	开启	0
6	0	允许	关闭	关闭	关闭	关闭	开启	0
7	0	允许	关闭	关闭	关闭	关闭	开启	0
8	0	允许	关闭	关闭	关闭	关闭	开启	0
9	0	允许	关闭	关闭	关闭	关闭	开启	0
10	0	允许	关闭	关闭	关闭	关闭	开启	0
11	0	允许	关闭	关闭	关闭	关闭	开启	0
12	0	允许	关闭	关闭	关闭	关闭	开启	0

## 2)、速率限制:

速率限制 ID: 限速编号,

速率: 可配置范围[0-131071], pps 每秒转发报文个数

- 系统配置
- 端口配置
- ▾ 网络安全
  - 端口安全
  - 端口隔离
  - ▾ ACL
    - 端口
    - 速率限制
    - 访问控制列表
- 聚合
- 环路保护
- 生成树

ACL速率限制配置

速率限制 ID	速率 (pps)
*	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1

## 3)、访问控制列表:

- 系统配置
- 端口配置
- ▾ 网络安全
  - 端口安全
  - 端口隔离
  - ▾ ACL
    - 端口
    - 速率限制
    - 访问控制列表
- 聚合
- 环路保护
- 生成树
- IP Source Guard
- ARP 检查
- DHCP 探测配置
- IGMP 监听

访问控制列表配置

入端口	Policy / Bitmask	帧类型	处理模式	速率限制	复制到端口	Port Redirect	帧数量
+							

点击蓝色  进入 ACE 配置页面；该页面可添加 acl 表项

## ACE配置

Ingress 端口	All	▼
策略筛选	所有	▼
Frame 类型	所有	▼

处理模式	允许	▼
速率限制	关闭	▼
重定向到端口	关闭	▼
记录Log	关闭	▼
关闭端口	关闭	▼
帧数量	0	

## MAC参数

DMAC过滤	所有	▼
--------	----	---

## VLAN参数

VLAN ID过滤	所有	▼
标签优先级	所有	▼

一条 ACL 表项有一些参数组成，选择的 Frame 类型不一样，给出参数也不同：

入端口： 可选择该 ACE 应用到指定特定的端口，还是应用到全部端口

策略过滤： 为该 ACL 表项“指定”策略过滤编号和掩码或“所有” “所有”表示：不关心，没有过滤策略；

策略编号： 0-255

策略掩码： 0x0 - 0xff

## Frame 类型：

“所有”：所有的帧都匹配该 ACE

“以太网类型”：匹配大于 0x600 以太网 Length/Type

“ARP”： 仅匹配 ARP 帧，不会再匹配以太网类型

“IPV4”： 仅匹配 IPV4 帧，不会再匹配以太网类型

### ① 选择“以太网类型”

## MAC参数

SMAC过滤	所有	▼
DMAC过滤	所有	▼

## VLAN参数

VLAN ID过滤	所有	▼
标签优先级	所有	▼

## 以太网类型参数

EtherType过滤	所有	▼
-------------	----	---

② 选择“ARP”

### MAC 参数

SMAC 过滤	所有	▼
DMAC 过滤	所有	▼

### VLAN 参数

VLAN ID 过滤	所有	▼
标签优先级	所有	▼

### ARP 参数

ARP/RARP	所有	▼
请求/应答	所有	▼
发送IP过滤	所有	▼
目标IP过滤	所有	▼

ARP源MAC匹配	所有	▼
RARP目标MAC匹配	所有	▼
IP/以太网范围	所有	▼
IP	所有	▼
以太网	所有	▼

保存 重置 取消

③ 选择“IPV4”

### MAC 参数

DMAC 过滤	所有	▼
---------	----	---

### VLAN 参数

VLAN ID 过滤	所有	▼
标签优先级	所有	▼

### IP 参数

IP协议过滤	所有	▼
IP TTL	所有	▼
IP分段	所有	▼
IP选项	所有	▼
SIP过滤	所有	▼
DIP过滤	所有	▼

保存 重置 取消

## 4)、MAC 参数说明:

### 源 mac 过滤: (以太网类型和 arp 类型支持)

“所有”: 表示不关心, “指定”: 可以配置一个过滤的的源 mac 地址

格式: “xx-xx-xx-xx-xx-xx” or “xx.xx.xx.xx.xx.xx” or “xxxxxxxxxxxx”

### 目的 mac 过滤:

“所有”: 表示不关心,

“MC”: 组播

“BC”: 广播

“UC”: 单播

“指定”: 可以配置一个过滤的的目的 mac 地址

## 5)、VLAN 参数说明:

Vlan id 过滤: 可以指定某个 vlan, 或不关心

Tag 优先级: 0-7 或任意

## 6)、以太网类型参数说明:

以太网类型过滤: 指定一个类型值或不关心

## 7)、ARP 参数:

ARP/RARP

## 8)、请求/应答:

指定请求还是应答报文过滤

## 9)、发送 IP 过滤:

可以指定是某台主机或某一网段

## 10)、目的 IP 过滤:

可以指定是某台主机或某一网段

## 11)、ARP 源 mac 匹配:

0: ARP 报文发送硬件地址 (SHA) 与 SMAC 不相等

1: ARP 报文发送硬件地址 (SHA) 与 SMAC 相等

## 12)、RARP 目的 mac 匹配:

0: RARP 报文目标硬件地址 (THA) 与 SMAC 不相等

1: RARP 报文目标硬件地址 (THA) 与 SMAC 相等

## 13)、IP/以太网长度:

0: 硬件地址长度不为 6 或协议地址长度不为 4

1: 硬件地址长度不为 6 且协议地址长度不为 4

## 14)、以太网硬件地址类型:

0: 不等于 1

1: 等于 1

## 15)、IP 协议地址类型:

0: 不等于 0x800

1: 等于 0x800

## 16)、IP 参数说明:

### ① 、IP 协议过滤:

ICMP、UDP、TCP、其他

#### IP 参数

IP 协议过滤	ICMP
IP TTL	所有
IP 分段	所有
IP 选项	所有
SIP 过滤	所有
DIP 过滤	所有

保存 重置 取消

#### ICMP Parameters

ICMP 类型过滤	所有
ICMP 代码过滤	所有

### ② 、选择其它需要指定协议字段值 [0-255]

#### a. IP TTL:

zero: ipv4 报文中 ttl 大于 0 且不能匹配这表项

non-zero: ipv4 报文中 ttl 大于 0 且匹配这表项

#### b. IP 分组:

#### c. IP 选项

#### d. 源 IP 过滤

可以指定是某台主机或某一网段

#### e. 目的 IP 过滤

可以指定是某台主机或某一网段

## 16)、ICMP 参数说明:

### ① ICMP 类型过滤

可以指定类型值 0-255

#### IP 参数

IP 协议过滤	UDP
IP TTL	所有
IP 分段	所有
IP 选项	所有
SIP 过滤	所有
DIP 过滤	所有

保存 重置 取消

#### UDP Parameters

源端口过滤	指定
源端口号	0
目的端口过滤	范围
目的端口范围	0 - 65535

### ② ICMP code 过滤

可以指定 code 值 0-255

## IP 参数

IP 协议过滤	TCP
IP TTL	所有
IP 分段	所有
IP 选项	所有
SIP 过滤	主机
SIP 地址	192.168.10.1
DIP 过滤	网络
DIP 地址	192.168.8.1
DIP 掩码	255.255.255.0

保存 重置 取消

## TCP Parameters

源端口过滤	指定
源端口号	0
目的端口过滤	范围
目的端口范围	0 - 65535
TCP FIN	0
TCP SYN	1
TCP RST	所有
TCP PSH	所有
TCP ACK	所有
TCP URG	所有

## 17)、TCP/UDP 参数说明:

### ① 源端口过滤:

可以指定具体某一个 0-65535

也可以指定一个范围

### ② 目的端口过滤

可以指定具体某一个 0-65535

也可以指定一个范围

### ③ TCP 相关的 FLAGS: 都可以指定

TCP FIN、TCP SYN、TCP RST、TCP PSH、TCP ACK、TCP URG

## 13、聚合

### 1)、静态聚合:

**端口成员:** 端口加入聚合必须是相同的 speed 和全双工;

此交换机支持32组汇聚, 每组支持最多8个端口。配置汇聚组只需将汇聚的端

口点击选择到同一行组号即可, 如图21所示: 1-2 口一组汇聚; 3-4 口一组汇聚等。汇聚组

成员端口请保持配置一致性, 如端口速率模式、所属vlan 信息等。

链路汇聚的负载均衡模式支持:

“源MAC 地址”(基于报文的源MAC 地址进行负载均衡计算)

“目的MAC 地址”(基于报文的源MAC 地址进行负载均衡计算)、

“IP 地址”(将报文的源IP 地址和目的IP 地址进行异或之后再行负载均衡计算)、

“TCP/UDP 端口号”(基于报文的TCP/UDP 端口号进行负载均衡计算)。

四种模式可复选, 组合计算。均衡算法的指定是全局性的;

如果某些端口已开启LACP 动态汇聚协议, 则无法手工配置静态汇聚。

**注意:** 同一端口静态汇聚不能与动态LACP 汇聚同时配置

- ▶ 系统配置
- ▶ 端口配置
- ▶ 网络安全
- ▼ 聚合
  - 静态
  - 动态
- ▶ 环路保护
- ▶ 生成树
- ▶ IP Source Guard
- ▶ ARP 检查
- ▶ DHCP探测配置
- ▶ IGMP 监听
- ▶ MAC 地址表
- ▶ VLANs配置
- 镜像
- 堆叠

## 聚合模式配置

负载均衡模式	
源MAC地址	<input checked="" type="checkbox"/>
目的MAC地址	<input type="checkbox"/>
IP地址	<input checked="" type="checkbox"/>
TCP/UDP端口号	<input checked="" type="checkbox"/>

## 链路聚合配置 for Switch 1

组ID	端口成员																											
	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
普通模式	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>																							
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
9	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
10	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
11	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
12	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## 2)、动态聚合:

此交换机支持端口动态汇聚，端口开启动态协议以后，汇聚的双方设备通过协

议交互汇聚信息，根据双方的参数和状态，自动将匹配的链路汇聚在一起收发数据。汇聚

形成后，交换设备维护汇聚链路状态，当双方配置变化时，自动调整或解散汇聚链路。

动态协议的配置参数包括协议开关状态和协商密钥及主动被动模式选择。只有开启

动态协议的端口才会进行动态协商，从而有可能形成汇聚链路。密钥是协商的基础，

具有相同密钥的端口才能协商组成一个汇聚链路。协商模式“active|passive”，当选择

“active”，设备会主动发起汇聚协商；当选择“passive”，设备被动接受其他设备发起的汇聚协商。如果某些端口已经进行了静态的端口汇聚，可无法实现LACP 动态汇聚。

**注意：**同一端口动态 LACP 汇聚不能与静态汇聚同时配置

- ▶ 系统配置
- ▶ 端口配置
- ▶ 网络安全
- ▼ 聚合
  - 静态
  - 动态
- ▶ 环路保护
- ▶ 生成树
- ▶ IP Source Guard
- ▶ ARP 检查
- ▶ DHCP探测配置
- ▶ IGMP 监听
- ▶ MAC 地址表
- ▶ VLANs配置
- 镜像
- 堆叠

## 动态链路聚合端口配置 for Switch 1

端口	动态开启	Key	Role	Timeout	Prio
*	<input type="checkbox"/>	<>	<>	<>	32768
1	<input type="checkbox"/>	Auto	Active	Fast	32768
2	<input type="checkbox"/>	Auto	Active	Fast	32768
3	<input type="checkbox"/>	Auto	Active	Fast	32768
4	<input type="checkbox"/>	Auto	Active	Fast	32768
5	<input type="checkbox"/>	Auto	Active	Fast	32768
6	<input type="checkbox"/>	Auto	Active	Fast	32768
7	<input type="checkbox"/>	Auto	Active	Fast	32768
8	<input type="checkbox"/>	Auto	Active	Fast	32768
9	<input type="checkbox"/>	Auto	Active	Fast	32768
10	<input type="checkbox"/>	Auto	Active	Fast	32768
11	<input type="checkbox"/>	Auto	Active	Fast	32768
12	<input type="checkbox"/>	Auto	Active	Fast	32768

## 14、环路保护

### 全局配置:

开启环路保护: 默认关闭默认关闭; 开启后可以对设备环路(自环)进行检测;

发送时间: 发送 PDU 环路检查时间间隔; [1-10s], 默认 5s

关闭时间: 端口 disable 的持续时间[0-604800s], 0 表示一直关闭到设备重启, 最长为 7 天; 默认 180s 基于端口配置

### 端口下开启:

ACTION: 检查到环路可执行 3 种操作:

disable 端口:

disable 端口以及 log 记录;

记录 log;

Tx Mode: 配置端口是 active 主动发送环路 PDU 还是 Passive 接收环路包



### Loop Protection Configuration

常规设置			
全局配置			
开启环路保护	关闭		
发送时间	5	秒	
关闭时间	180	秒	

端口配置 for Switch 1			
端口	启动	动作	发送PDU侦测包
*	<input checked="" type="checkbox"/>	<>	<>
1	<input checked="" type="checkbox"/>	关闭端口	启动
2	<input checked="" type="checkbox"/>	关闭端口	启动
3	<input checked="" type="checkbox"/>	关闭端口	启动
4	<input checked="" type="checkbox"/>	关闭端口	启动
5	<input checked="" type="checkbox"/>	关闭端口	启动
6	<input checked="" type="checkbox"/>	关闭端口	启动
7	<input checked="" type="checkbox"/>	关闭端口	启动
8	<input checked="" type="checkbox"/>	关闭端口	启动

## 15、生成树

### 1)、桥配置:

协议版本: 默认开启的是 RSTP;

桥优先级: 越小越优先, 可用于选择根桥

转发延迟: 根端口和指定端口转发延迟时间; 配置范围[4-30s]

最大 Age: 当为跟桥时, 发送信息最大超时时间; 配置范围[6-40s] 必须满足 最大 Age 时间  $\leq$  (转发延迟时间 - 1) \* 2

最大跳数: MSTP中使用, 当跳数为 0 则表示该BPDU信息超时, 设备收到Hops值为 0 的BPDU 就要丢弃它。可配置范围[6-40]

发送 HOLD 计数: 桥端口每秒发送 BPDU 个数, 可配置范围[1-10];

## 2)、高级配置:

**边缘端口 BPDU 过滤:** 边缘端口不处理 BPDU 报文, 不参与拓扑的计算

**边缘端口BPDU保护:** 边缘端口收到了BPDU, 该端口就会进入Error-disabled 状态, 以示配置错误; 同时整个端口被关闭, 表示网络中可能被非法用户增加了一台网络设备, 使网络拓扑发生改变。

**端口错误恢复:** 是否允许Error-disabled 状态端口自动恢复;

**端口错误恢复超时:** Error-disabled 状态端口恢复的超时时间, 配置范围[30 -86400]

- ▶ 系统配置
- 端口配置
- ▶ 网络安全
- ▶ 聚合
- 环路保护
- ▼ 生成树
  - 桥配置
  - CIST 端口配置
- ▶ IP Source Guard
- ▶ ARP 检查
- DHCP 探测配置
- ▶ IGMP 监听
- MAC 地址表
- VLANs 配置
- 镜像
- 堆叠

### STP 桥配置

**基本设置**

协议版本	MSTP
网桥优先级	32768
转发延迟	15
Max Age	20
最大跳数	20
Transmit Hold Count	6

**高级设置**

端口BPDU过滤	<input type="checkbox"/>
端口BPDU保护	<input type="checkbox"/>
端口错误恢复	<input type="checkbox"/>
端口错误恢复超时	<input style="width: 100%;" type="text"/>

保存
重置

## 3)、CIST 端口配置:

**端口路径开销:** 默认为自动计算, 用户也可手工指定, 开销值 (1-20000000) 之间, 值越小路径越优先。

**端口优先级:** 在生成树计算过程中使用, 可配置 (0/16/32/48/.../224/240), 默认为128。

**边缘端口:** 当交换机连接电脑或者没有生成树功能的网络设备时使用。此时端口直接进入转发状态, 不会参与RSTP 逻辑拓扑计算。

**非根端口:** 可配置交换机的所有端口为“非根端口”或“根端口”, 进而改变生成树拓扑。限制拓扑更改, 端口可选择强制拓扑不更改, 或不强制。

所有端口可开启“BPDU 保护”来保持网络稳定。

对于设备之间互连, 可指定链路为点到点类型, 或非点到点类型, 从而减少生成树计算。

- ▶ 系统配置
- ▶ 端口配置
- ▶ 网络安全
- ▶ 聚合
- ▶ 环路保护
- ▶ 生成树
  - 桥配置
  - CIST 端口配置
- ▶ IP Source Guard
- ▶ ARP 检查
- ▶ DHCP 探测配置
- ▶ IGMP 监听
- ▶ MAC 地址表
- ▶ VLANs 配置
- ▶ 镜像
- ▶ 堆叠

## STP CIST 端口配置

CIST 聚合端口配置										
端口	STP 开启	Path Cost	优先权	管理 Edge	Auto Edge	限制作用	TCN	BPDU 防护	Point-to-point	
-	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	强制 True	

CIST 正常端口配置 for Switch 1										
端口	STP 开启	Path Cost	优先权	管理 Edge	Auto Edge	限制作用	TCN	BPDU 防护	Point-to-point	
*	<input type="checkbox"/>	<>	<>	<>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>	
1	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
2	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
3	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
4	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
5	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
6	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
7	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
8	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
9	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
10	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	
11	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	

## 4)、IP Source Guard

通过 IP Source Guard 绑定功能，可以对端口转发的报文进行过滤控制，防止非法报文通过端口，从而限制了对网络资源的非法使用（比如非法主机假冒合法用户 IP 接入网络），提高了端口的安全性。

**配置：**指定可在给定的端口上学习到的动态客户端的最大数量。这个值可以是 0，1，2 或无限的。如果端口模式被激活，最大动态客户端的值等于 0，则表示只允许被匹配在特定端口上的静态项中的 IP 数据包的转发。

- ▶ 系统配置
- ▶ 端口配置
- ▶ 网络安全
- ▶ 聚合
- ▶ 环路保护
- ▶ 生成树
- ▶ IP Source Guard
  - 配置
  - 静态表项配置
- ▶ ARP 检查
- ▶ DHCP 探测配置
- ▶ IGMP 监听
- ▶ MAC 地址表
- ▶ VLANs 配置
- ▶ 镜像
- ▶ 堆叠

## IP Source 保护配置

模式

动态转静态

## 端口模式配置 for Switch 1

端口	模式	最大动态客户端
*	<>	<>
1	关闭	无限制
2	关闭	无限制
3	关闭	无限制
4	关闭	无限制
5	关闭	无限制
6	关闭	无限制

## 5)、静态表项配置：

删除：检查要删除的条目；

端口：选择配置的端口号；

VLAN ID：填写配置的 VLAN ID 号；

IP 地址：输入配置的 IP 地址；

IP 掩码：输入配置 IP 地址相应的掩码；

- ▶ 系统配置
- ▶ 端口配置
- ▶ 网络安全
- ▶ 聚合
- ▶ 环路保护
- ▶ 生成树
- ▶ IP Source Guard
  - 配置
  - 静态表项配置
- ▶ ARP 检查
- ▶ DHCP探测配置

静态IP Source表for Switch 1

删除	端口	VLAN ID	IP 地址	IP掩码
删除	1			

添加新表项

保存 重置

## 16、ARP 检查

### 1)、配置:

指定ARP检测是哪个端口上启用。只有当这两个全局配置模式和端口模式给定的端口上启用，ARP检测是这个给定端口上启用。可能的模式有:

**启用:** 启用ARP检测操作。

**已禁用:** 禁用ARP检测操作。

如果你想检查VLAN配置，您必须启用“检查VLAN”的设置。“检查的VLAN”的默认设置为禁用。当“检查VLAN”的设置被禁用，ARP检测的日志类型将引用的端口设置。和“检查VLAN”的设置被启用，ARP检测的日志类型将参照VLAN设置。“检查的VLAN”的可能设置是:

**启用:** 启用核VLAN操作。

**已禁用:** 禁用检查VLAN操作。

只有全局配置模式和端口模式给定的端口上启用，并且“检查VLAN”的设置被禁用，ARP检测的日志类型将引用的端口设置。有四种日志类型和可能的类型是:

**无:** 不配置。**拒绝:** 拒绝日志条目。**允许:** 登录许可项目。**所有:** 日志中的所有条目。

- ▶ 系统配置
- ▶ 端口配置
- ▶ 网络安全
- ▶ 聚合
- ▶ 环路保护
- ▶ 生成树
- ▶ IP Source Guard
- ▶ ARP 检查
  - 配置
  - VLAN配置
  - 静态表项配置
  - 动态表项
- ▶ DHCP探测配置
- ▶ IGMP监听
- ▶ MAC 地址表
- ▶ VLANs配置
- ▶ 镜像
- ▶ 堆叠

ARP检查配置

模式 关闭

动态转静态

端口模式配置for Switch 1

端口	模式	VLAN检查	Log类型
*	<>	<>	<>
1	关闭	关闭	无
2	关闭	关闭	无
3	关闭	关闭	无
4	关闭	关闭	无
5	关闭	关闭	无
6	关闭	关闭	无
7	关闭	关闭	无
8	关闭	关闭	无

### 2)、ARP 检测 vlan 配置

指定ARP检测被启用上的VLAN。首先，你必须启用端口模式配置网页端口设置。只有当这两个全局配置模式和端口模式给定的端口上启用，ARP检测是这个给定端口上启用。其次，你可以指定哪个VLAN将在VLAN模式配置网页进行检查。日志类型也可以对每个VLAN的设置进行配置。

**可能的类型包括：**

**无：** 不配置。

**拒绝：** 拒绝日志条目。

**允许：** 登录许可项目。

**所有：** 日志中的所有条目。

- ▶ 系统配置
- ▶ 端口配置
- ▶ 网络安全
- ▶ 聚合
- ▶ 环路保护
- ▶ 生成树
- ▶ IP Source Guard
- ▼ ARP 检查
  - 配置
  - VLAN配置
  - 静态表项配置
  - 动态表项
- ▶ DHCP探测配置

**VLAN模式配置**

开始从VLAN  显示  每页显示条目.

删除	VLAN ID	Log类型
删除	<input type="text"/>	无

**3)、静态表项配置：**

**删除：** 检查要删除的条目；将本条目删除；

**端口：** 选择将要配置相应的端口号；

**VLAN ID：** 选择将要配置相应的VLAN ID号；

**MAC地址：** 允许源MAC地址的ARP请求报文；

**IP地址：** 在ARP请求报文允许源IP地址。

- ▶ 系统配置
- ▶ 端口配置
- ▶ 网络安全
- ▶ 聚合
- ▶ 环路保护
- ▶ 生成树
- ▶ IP Source Guard
- ▼ ARP 检查
  - 配置
  - VLAN配置
  - 静态表项配置
  - 动态表项

**静态ARP检查表for Switch 1**

删除	端口	VLAN ID	MAC地址	IP 地址
删除	1	<input type="text"/>	<input type="text"/>	<input type="text"/>

**4)、动态表项：**

每个页面都显示了动态 ARP 检测表多达 99 项，默认为 20，通过“每页的条目”输入字段中选择。当第一次访问，网页会显示前 20 项由动态 ARP 检测表的开始。

在“从端口地址开始”，“VLAN”，“MAC 地址”和“IP 地址”输入字段允许用户选择在动态 ARP 检测表的起点。单击该按钮将更新从该表显示启动或最接近的下一个动态 ARP 检测表匹配。此外，两个输入字段将 - 在点击一个按钮 - 假设第一个显示条目的值，允许连续刷新具有相同的起始地址。

在将使用当前显示的表中的最后一个条目为下次查找的基础。当最终到达文本“没有更多的条目”显示在显示表。使用按钮重新开始。

## 17、DHCP 探测配置

此页面配置 DHCP 探测功能：

**启用：**启用 DHCP Snooping 功能模式运行。如果启用了 DHCP Snooping 功能模式下运行时，DHCP 请求报文将被转发到信任端口，只允许来自信任端口应答报文。

**已禁用：**禁用 DHCP Snooping 功能模式运行。

端口	模式
*	<>
1	信任
2	信任
3	信任
4	信任
5	信任
6	信任
7	信任

## 18、IGMP 监听

### 1)、基本配置:

**监听功能:** 开启“√”、默认关闭;

**启用 IPMCv4 功能:** 允许未注册 IPMCv4 信息的控制, 只有当 IGMP Snooping 已经启动的效果。当 IGMP Snooping 功能被禁用, 未注册 IPMCv4 流量始终是积极的, 尽管此设置。

**IGMP SSM 范围:** SSM (特定源组播) 范围允许 SSM 感知主机和路由器运行 SSM 服务模型组的地址范围。

**Leave Proxy 开启:** 开启“√”、默认关闭; 启用 IGMP 离开代理。此功能可用于避免不必要的转发离开报文的路由器侧。

**启用代理:** 启用 IGMP 代理。此功能可用于避免不必要的转发加入和离开消息到路由器侧。

**端口:** 所对应该的端口号;

**路由端口:** 指定哪些端口充当路由器端口。路由器端口的以太网交换机上的端口, 导致朝向三层组播设备或 IGMP 查询器。如果一个聚合成员端口被选择作为一个路由器端口, 整个聚合将作为一个路由器端口。

**Fast Leave:** 启用该端口上的快速离开。

**节流:** 启用限制组播组到该交换机端口可用数。

- ▶ 系统配置
- ▶ 端口配置
- ▶ 网络安全
- ▶ 聚合
- ▶ 环路保护
- ▶ 生成树
- ▶ IP Source Guard
- ▶ ARP 检查
- ▶ DHCP 探测配置
- ▶ IGMP 监听
  - 基本配置
  - VLAN 配置
  - MAC 地址表
  - VLANs 配置
  - 镜像
  - 堆叠

#### 组播侦听配置

全局配置	
监听功能	<input type="checkbox"/>
启用 IPMCv4 功能	<input checked="" type="checkbox"/>
IGMP SSM 范围	232.0.0.0 / 8
Leave Proxy 开启	<input type="checkbox"/>
启用代理	<input type="checkbox"/>

#### 端口配置 for Switch 1

端口	路由端口	Fast Leave	节流
*	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

### 2)、VLAN 配置:

**删除:** 检查要删除的条目;

**VLAN ID:** 选择将要配置相应的 VLAN ID 号;

**监听功能:** 使每个 VLAN 的 IGMP Snooping 功能。多达 32 个 VLAN 可以选择 IGMP Snooping 功能。

**IGMP 查询:** 加入 IGMP 查询选取中的 VLAN。

**兼容性:** 兼容性是由主机和路由器采取适当的行动取决于 IGMP 协议在网络中的主机和路由器操作系统版本保持。

**PRI:** 允许选择是 IGMP-自动, 强制 IGMPv1 中, 强制 IGMPv2 的, 强制的 IGMPv3, 默认兼容性值是 IGMP 的设备;

**RV:** 优先级接口。它表示由该系统产生的 IGMP 控制帧的优先级。这些值可以被用来优先不同类别的通信量。允许的范围

是 0（尽力而为）到 7（最高），默认的接口优先级值是 0。

**Q1:**允许的范围是 1 到 255，默认的系数为 2。

**QRI:**查询时间间隔。查询间隔是由查询器发送通用查询的间隔。允许的范围是 1 到 31744 秒，默认查询间隔为 125 秒。

**LLQ1:**查询响应间隔。最大响应时间来计算插入的周期性一般查询的最大响应代码。允许的范围是 0 到 31744 以十分之一秒，默认的查询响应间隔以秒（10 秒）十分之一 100。

**URI:**最后成员查询间隔。最后成员查询时间是最后成员查询时间间隔，再乘以最后成员查询计数表示的时间值。允许的范围是 0 到 31744 以十分之一秒，默认最后成员查询间隔为 10 秒（1 秒）十分之一。

- 系统配置
- 端口配置
- 网络安全
- 聚合
- 环路保护
- 生成树
- IP Source Guard
- ARP 检查
- DHCP 探测配置
- ▾ IGMP 监听
  - \* 基本配置
  - \* VLAN 配置

#### IGMP SNOOPING VLAN 配置

起始 VLAN  到  每页条目.

删除	VLAN ID	监听功能	IGMP 查询	兼容性	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
----	---------	------	---------	-----	-----	----	----------	---------------	----------------	-----------

添加新的 IGMP VLAN

保存 重置

## 19、MAC 地址表

显示 MAC 地址表配置页面；此页面上配置 MAC 地址表。设置动态 MAC 地址表中的条目，并配置静态 MAC 地址表。

- 系统配置
- 端口配置
- 网络安全
- 聚合
- 环路保护
- 生成树
- IP Source Guard
- ARP 检查
- DHCP 探测配置
- IGMP 监听
- MAC 地址表
- VLANs 配置
- 镜像
- 堆叠

#### MAC 地址配置

##### 老化配置

禁止自动老化

老化时间  秒

##### MAC 地址学习 for Switch 1

	端口成员																												
	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	
Auto	<input checked="" type="checkbox"/>																												
关闭	<input type="checkbox"/>	<input type="checkbox"/>																											
安全	<input type="checkbox"/>	<input type="checkbox"/>																											

##### 静态 MAC 地址配置 for Switch 1

删除	VLAN ID	MAC 地址	端口成员																										
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23				
删除	1	00-00-00-00-00-00	<input type="checkbox"/>																										

添加新的地址条目

## 20、VLAN5 配置

**存在 VLANs:** 此字段显示了在交换机上的所有交换机创建的 VLAN。

默认情况下，只有 VLAN1 的存在。多个 VLAN 可以使用列表语法，其中的各个元素之间用逗号分隔来创建。范围指定用破折号分隔的下限和上限。

下面的例子将创建 **VLAN1, 10, 11, 12, 13, 200, 和 300: 1,10-13,200,300**。空格是允许的分隔符之间。

**端口:** 显示端口对应的端口号;

**模式:** 端口模式（默认为 Access）确定端口问题的基本行为。一个端口可以有三种模式，如下所述之一。只要选择一个特定的模式，在该行的其余字段将要么变灰或者根据所对应的模式下进行变更。变灰字段显示的值，该端口将得到当模式被应用。

### 1)、Access:

接入端口通常用于连接到终端站。如语音 VLAN 的动态特性可以添加端口到幕后多个 VLAN。接入端口，具有以下特点:

- ✓ 只有一个 VLAN，端口 VLAN（又名接入 VLAN），默认情况下为 1 的成员，
- ✓ 接受未标记的帧和 C-标记的帧，
- ✓ 丢弃未分类的访问 VLAN 中的所有帧，
- ✓ 对出口的所有帧被发送未标记。

### 2)、Trunk:

Trunk 端口可以同时进行多个 VLAN 的流量，并通常用于连接到其他交换机。Trunk 端口具有以下特点:

- ✓ 默认情况下，Trunk 端口是所有现有 VLAN 的成员。这可以通过使用允许的 VLAN 是有限的，
- ✓ 除非 VLAN 中继的端口上启用，划分到不同的 VLAN，该端口是不是成员的帧将被丢弃，
- ✓ 默认情况下，所有的帧，但归类到端口的 VLAN（也称为本地 VLAN）帧标记获取关于出口。归入到端口 VLAN 的帧没有得到 C-标记的出口，
- ✓ 出口标记可以改变标记的所有帧，在这种情况下，仅接受已标记帧的入口，
- ✓ VLAN 中继可能被启用。

### 3)、Hybrid:

Hybrid 端口类似于在许多方面 Trunk 端口，但增加了额外的端口配置功能。除了为中继端口描述的特征，Hybrid 端口具备这些能力:

- ✓ 可配置为 VLAN 标记或不知道，C-标记所有，S 标签所有，或 S-自定义标签所有，
- ✓ 入口过滤可以控制的，
- ✓ 进入验收帧出口标注和配置都可以独立配置。

### 4)、端口 VLAN:

确定端口的 VLAN ID（也称为 PVID）。允许的 VLAN 的范围是 1 到 4095，默认为 1。

### 5)、端口类型:

在混合模式端口允许更改端口类型，也就是一帧的 VLAN 标记是否被用来在入口的帧分类到特定的 VLAN，如果是这样，

这 TPID 它的反应上。同样，在出口处，端口类型决定了标签的 TPID，如果需要的标签。

## 6)、Unaware:

在入口处，所有的帧，是否携带 VLAN 标记或没有，得到归类到端口的 VLAN，而且可以标记不是在出口中删除。

## 7)、C-Port:

在入口处，帧带 VLAN 标记 TPID = 0x8100 的 GET 划分到 VLAN ID 内嵌标签。如果一帧标记的未标记或优先级，该框架被归类到端口的 VLAN。如果帧必须被标记的出口，他们将被标记为一个 C 标记。

## 8)、S -Port:

在入口处，帧与 TPID = 0x8100 或 0x88A8 得到归类到的 VLAN ID 嵌入在标签的 VLAN 标签。如果一帧标记的未标记或优先级，该框架被归类到端口的 VLAN。如果帧必须被标记的出口，他们将被标记为 S -标签。

## 9)、S-Custom-Port:

在入口处，帧与一个 TPID = 0x8100 或等于配置的自定义-S 端口得到归类到的 VLAN ID 嵌入在标签的以太网类型的 VLAN 标签。如果一帧标记的未标记或优先级，该框架被归类到端口的 VLAN。如果帧必须被标记的出口，他们将被标记为自定义 S 标签。

## 10)、输入过滤:

- ✓ Hybrid 端口允许改变入口过滤。接入和中继端口始终启用入口过滤。
- ✓ 如果入口过滤功能（复选框被选中），帧划分到一个 VLAN 中的端口是不是被丢弃的成员。
- ✓ 如果入口过滤被禁用，归入到一个 VLAN 中的端口不是成员帧被接受并转发到交换机引擎。然而，该端口将不会传输分类为 VLAN 的帧，它不是成员。

## 11)、VLAN Trunking:

- ✓ Trunk 端口和 Hybrid 端口允许启用 VLAN 中继。
- ✓ 当 VLAN 中继启用，归入未知 VLAN 的帧被接受该端口入口过滤是否启用或禁用。
- ✓ 这是在设备中交换机必须符合尚未创建的 VLAN 有用。通过配置连接交换机的中继端口的云的端口，就可以无缝地进行这些 VLAN 从一端到另一端。

## 12)、入口接收:

- ✓ Hybrid 端口允许改变帧上被接受进入的类型。
- ✓ Tagged and Untagged:
- ✓ 标记和非标记帧被接受。
- ✓ Tagged Only:
- ✓ 仅接受已标记帧的入口。未标记的帧将被丢弃。
- ✓ Untagged Only:
- ✓ 只有未标记的帧被接受的入口。标记的帧将被丢弃。

### 13)、出口 tag:

- ✓ 在 Trunk 端口和 Hybrid 模式的端口可以控制帧对出口的标记。

#### Untag Port VLAN:

- ✓ 归入到端口的 VLAN 帧传输未标记。其他帧发送相关标签。

#### Tag All:

- ✓ 所有帧，是否归入端口 VLAN 与否，都发送一个标记。

#### Untag ALL:

- ✓ 所有帧，是否归入端口 VLAN 与否，都没有一个标签发送。
- ✓ 此选项仅适用于混合模式端口。

### 14)、允许 VLANS:

- ✓ 在 Trunk 端口和 Hybrid 模式的端口可以控制他们被允许的 VLAN 成为会员。接入端口只能是一个 VLAN，接入的 VLAN 成员。
- ✓ 该字段的语法是相同的，在现有的 VLAN 领域中使用的语法。默认情况下，端口可能成为所有可能的 VLAN 的成员，并因此设置为 1-4095。
- ✓ 该字段可以为空，这意味着该端口将不被任何现有的 VLAN 的成员，但如果它被配置为 VLAN 中继它仍然能够承载所有未知的 VLAN。

### 15)、禁止 VLANS:

- ✓ 一个端口可被配置成永远是一个或多个 VLAN 的成员。这是当像 MVRP 和 GVRP 动态 VLAN 协议必须从动态添加端口的 VLAN 来防止特别有用。
- ✓ 诀窍是为禁止端口的问题上，以纪念这样的 VLAN。语法是相同的，在现有的 VLAN 领域中使用的语法。
- ✓ 默认情况下，该字段为空，这意味着该端口可能成为所有可能的 VLAN 的成员。

- ▶ 系统配置
- ▶ 端口配置
- ▶ 网络安全
- ▶ 聚合
- ▶ 环路保护
- ▶ 生成树
- ▶ IP Source Guard
- ▶ ARP 检查
- ▶ DHCP 探测配置
- ▶ IGMP 监听
- ▶ MAC 地址表
- ▶ VLANs 配置
- ▶ 镜像
- ▶ 堆叠

#### 配置 VLAN 成员 for Switch 1

存在 VLANs	1
QINQ 以太帧类型	88A8

#### VLAN 端口配置

端口	模式	端口 VLAN	端口类型	输入过滤	VLAN Trunking	入口接收	出口 tag	允许 VLANs	禁止 VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged and Untagged	Untag All	1	

## 21、镜像

显示镜像配置页面，此页面用来配置镜像。

**目的端口：** 将某些端口的业务或者控制报文流量完整地映射到指定的端口；

**镜像端口：** 被映射的端口

**接收：** 只接收不发送；**发送：** 只发送不接收；**接收与发送：** 即接收也发送。



## 22、堆叠

**堆叠状态：** 堆叠显示当前是否启用或禁用。

**开启堆叠：** 此项是开启或关闭堆叠功能；默认是关闭的。当更改此项设置，必须重新启动设备生效。

**删除：** 删除堆叠中的成员配置；

**堆叠成员：** 堆叠成员中显示交换机的 MAC 地址；

**Switch ID：** 显示堆叠成功后堆叠成员的显示 ID；也可在堆叠成功后进行修改；

**Capable：** 此功能显示是否成为主控；

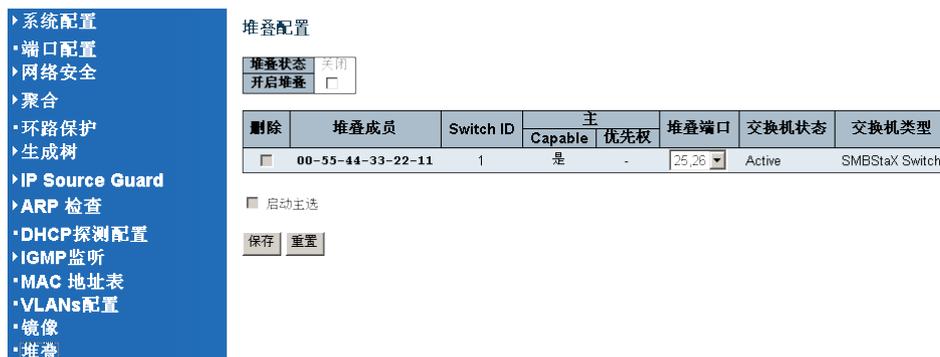
**优先权：** 交换机主选进程的优先级。越小越有可能在主选过程中成为主选；

**堆叠端口：** 一对端口用于连接到堆叠中的其他交换机。如果堆叠目前已启用，交换机必须重新启动新的堆叠端口才能生效。

**交换机状态：** 显示交换机目前存在于堆叠成员内的状态，如果需要重新启动配置进行了更改。

**交换机类型：** 交换机产品的名称；

**示例：** 将开启堆叠选取；点击保存即可开启堆叠功能！



## 三、设备状态

### 1、系统

1)、**信息**：显示系统联系方式、名称、位置；硬件 MAC 地址；系统日期、系统运行时间；软件版本、软件日期。

- ▼ 系统
  - 信息
  - CPU 负荷
  - IP 状态
  - 日志
  - 详细日志
  - 管理统计
- ▶ 端口
- ▶ 网络安全
- ▶ LACP
  - 环路保护
  - 生成树

#### 系统信息

系统	
<b>联系方式</b>	
名称	
位置	
硬件	
MAC 地址	00-55-44-33-22-11
时间	
系统日期	2013-12-17T16:06:17+08:00
系统运行时间	0d 06:51:18
软件	
软件版本	SMBStaX (stackable) 2013-12-16T10:47:35+08:00 R2.01
软件日期	2013-12-16T10:47:35+08:00

2)、**CPU 负荷**：显示当前设备 CPU 的运行负荷；

- ▼ 系统
  - 信息
  - CPU 负荷
  - IP 状态
  - 日志
  - 详细日志
  - 管理统计
- ▶ 端口
- ▶ 网络安全
- ▶ LACP

#### CPU 负荷

Your browser does not seem to support SVG.

3)、**IP 状态**：显示当前设备 IP 配置状态；

- ▼ 系统
  - 信息
  - CPU 负荷
  - IP 状态
  - 日志
  - 详细日志
  - 管理统计
- ▶ 端口
- ▶ 网络安全
- ▶ LACP
  - 环路保护
  - 生成树
- ARP 检测列表
- IP Source Guard 列表
- DHCP 监听表
- ▶ IGMP Snooping
- MAC 地址表
- ▶ VLANs
- 堆叠

#### IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80:1::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	00-55-44-33-22-11	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.149/24	
VLAN1	IPv6	fe80:2::255:44ff:fe33:2211/64	

#### IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
192.168.0.0/24	VLAN1	<UP HW_RT>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

#### Neighbour cache

IP Address	Link Address
192.168.0.1	VLAN1:00-3c-50-10-0a-30
192.168.0.151	VLAN1:30-85-a9-9f-88-e3
fe80:2::255:44ff:fe33:2211	VLAN1:00-55-44-33-22-11

4)、**日志**：显示系统日志信息；此页面查看系统信息、警告、错误信息、以及端口连接的状态；

- ▼ 系统
  - 信息
  - CPU负荷
  - IP状态
  - 日志
  - 详细日志
  - 管理统计
- ▶ 端口
- ▶ 网络安全
- ▶ LACP
  - 环路保护
  - 生成树

### 系统日志信息for Switch 1

级别	All
清除级别	All

消息的总数为 3 项。

起始ID  ,  每页显示的消息。

ID	undefined	时间	消息
1	Info	2013-12-17T09:15:10+08:00	Switch just made a cold boot.
2	Info	2013-12-17T09:15:11+08:00	Link up on switch 1, port 3
3	Info	2013-12-17T09:15:11+08:00	Link up on switch 1, port 19

**详细日志**：显示设备的级别、时间、消息；

- ▼ 系统
  - 信息
  - CPU负荷
  - IP状态
  - 日志
  - 详细日志
  - 管理统计
- ▶ 端口
- ▶ 网络安全
- ▶ LACP
  - 环路保护
  - 生成树

### 详细的系统日志信息for Switch 1

ID	<input type="text" value="1"/>
----	--------------------------------

#### Message

级别	Info
时间	1970-01-01T08:00:06+08:00
消息	Switch just made a cool boot.

5)、**管理统计**：此页面提供访问管理的统计数据。

- ▼ 系统
  - 信息
  - CPU负荷
  - IP状态
  - 日志
  - 详细日志
  - 管理统计
- ▶ 端口
- ▶ 网络安全
- ▶ LACP
  - 环路保护
  - 生成树
- ARP检测列表

### 访问管理统计

接口模块	接收数据包	允许数据包	丢弃数据包
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

## 2、端口

1)、**状态**：显示所有端口的连接状态；

- ▶ 系统
- ▶ 端口
  - 状态
  - 端口统计
  - 详细统计
- ▶ 网络安全
- ▶ LACP
  - 环路保护
  - 生成树
- ARP 检测列表
- IP Source Guard 列表
- DHCP 监听表
- ▶ IGMP Snooping
- MAC 地址表
- ▶ VLANs
- 堆叠

端口概述



2)、端口统计：通过此页面可以查看包括数据包、字节数、错误包、报文数、分段包的数据：

- ▶ 系统
- ▶ 端口
  - 状态
  - 端口统计
  - 详细统计
- ▶ 网络安全
- ▶ LACP
  - 环路保护
  - 生成树
- ARP 检测列表
- IP Source Guard 列表
- DHCP 监听表
- ▶ IGMP Snooping
- MAC 地址表
- ▶ VLANs
- 堆叠

端口统计概述 for Switch 1

端口	数据包		字节数		错误包		报文数		分段包
	接收	发送	接收	发送	接收	发送	接收	发送	
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	3633577	33817	464282737	4308195	0	0	0	239	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	34051	3622239	4395865	463987149	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0

3)、详细统计：此页面查看端口统计数据的各种数据包；

- ▶ 系统
- ▶ 端口
  - 状态
  - 端口统计
  - 详细统计
- ▶ 网络安全
- ▶ LACP
  - 环路保护
  - 生成树
- ARP 检测列表
- IP Source Guard 列表
- DHCP 监听表
- ▶ IGMP Snooping
- MAC 地址表
- ▶ VLANs
- 堆叠

详细端口统计 for Switch 1 Port 1

接收总数	
接收报文数	0
接收字节数	0
接收单播数	0
接收组播数	0
接收广播数	0
接收Pause帧	0
接收大小统计	
接收64字节大小报文数	0
接收65-127字节大小报文数	0
接收128-255字节大小报文数	0
接收256-511字节大小报文数	0
接收512-1023字节大小报文数	0
接收1024-1526字节大小报文数	0
接收1527-字节大小报文数	0
接收队列统计	
Rx Q0	0
Rx Q1	0
Rx Q2	0
Rx Q3	0
Rx Q4	0
Rx Q5	0
Rx Q6	0
Rx Q7	0
接收错误统计	
丢弃接收报文数	0

## 3、网络安全

此页面可以查看端口安全的安全状态、ACL 状态；

- ▶ 系统
- ▼ 端口
  - 状态
  - 端口统计
  - 详细统计
- ▼ 网络安全
  - ▼ 端口安全
    - Switch
    - 端口
  - ACL 状态
- ▶ LACP
  - 环路保护
- ▶ 生成树
- ARP 检测列表
- IP Source Guard 列表
- DHCP 监听表

### 端口安全状态

#### 用户协议显示

系统协议名称	Abbr
Limit Control	L
802.1X	8
DHCP Snooping	D
Voice VLAN	V

#### 端口状态 for Switch 1

端口	用户	状态	MAC地址数	
			当前	限制
1	----	关闭	-	-
2	----	关闭	-	-
3	----	关闭	-	-
4	----	关闭	-	-
5	----	关闭	-	-
6	----	关闭	-	-

- ▶ 系统
- ▼ 端口
  - 状态
  - 端口统计
  - 详细统计
- ▼ 网络安全
  - ▼ 端口安全
    - Switch
    - 端口
  - ACL 状态
- ▶ LACP

### 端口安全状态 for Switch 1 Port 1

MAC地址	VLAN ID	状态	添加时间	Age/Hold
没有MAC地址连接				

- ▶ 系统
- ▼ 端口
  - 状态
  - 端口统计
  - 详细统计
- ▼ 网络安全
  - ▼ 端口安全
    - Switch
    - 端口
  - ACL 状态
- ▶ LACP
  - 环路保护
- ▶ 生成树
- ARP 检测列表
- IP Source Guard 列表

### ACL 状态 for Switch 1

用户	入端口	帧类型	处理模式	速率限制	重定向到端口	CPU	CPU Once	帧数量	冲突
无项目									

## 1)、LACP

此页面显示所有的 LACP 实例的状态概览；包括系统状态、Port 状态、Port 统计；

- ▶ 系统
- ▶ 端口
- ▶ 网络安全
- ▼ LACP
  - 系统状态
  - Port 状态
  - Port 统计
  - 环路保护
- ▶ 生成树
- ARP 检测列表
- IP Source Guard 列表
- DHCP 监听表

LACP系统状态

Aggr ID	Partner 系统ID	Partner Key	Partner Prio	Last Changed	Local 端口
端口没有启用或没有成员					

- ▶ 系统
- ▶ 端口
- ▶ 网络安全
- ▼ LACP
  - 系统状态
  - Port 状态
  - Port 统计
  - 环路保护
- ▶ 生成树
- ARP 检测列表
- IP Source Guard 列表
- DHCP 监听表
- ▶ IGMP Snooping

LACP统计 for Switch 1

端口	LACP	Key	Aggr ID	Partner 系统ID	Partner 端口	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-
11	No	-	-	-	-	-
12	No	-	-	-	-	-
13	No	-	-	-	-	-

- ▶ 系统
- ▶ 端口
- ▶ 网络安全
- ▼ LACP
  - 系统状态
  - Port 状态
  - Port 统计
  - 环路保护
- ▶ 生成树

LACP 统计 for Switch 1

端口	LACP 接收	LACP 发送	丢弃	
			未知	非法
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0

## 2)、环路保护

此页面显示了环路保护的端口状态当前选择的交换机端口产生环路状态。

- ▶ 系统
- ▶ 端口
- ▶ 网络安全
- ▶ LACP
- ▶ 环路保护
- ▶ 生成树
- ▶ ARP检测列表
- ▶ IP Source Guard列表
- ▶ DHCP监听表

环路保护状态 for Switch 1

端口	动作	发送	环路	状态	循环	最后环路时间
没有端口启用						

### 3)、生成树

此页面显示生成树配置的桥状态、Port 状态、Port 统计：

- ▶ 系统
- ▶ 端口
- ▶ 网络安全
- ▶ LACP
- ▶ 环路保护
- ▶ 生成树
  - ▶ 桥状态
  - ▶ Port 状态
  - ▶ Port 统计
- ▶ ARP检测列表
- ▶ IP Source Guard列表
- ▶ DHCP监听表
- ▶ IGMP Snooping

生成树桥状态

MSTI	桥 ID	Root			拓扑标志	最后拓扑变化
		ID	Port	Cost		
CIST	32768.00-55-44-33-22-11	32768.00-55-44-33-22-11	-	0	Steady	-

### 4)、ARP 检测列表

此页面显示 ARP 检测配置列表：

- ▶ 系统
- ▶ 端口
- ▶ 网络安全
- ▶ LACP
- ▶ 环路保护
- ▶ 生成树
- ▶ ARP检测列表
- ▶ IP Source Guard列表
- ▶ DHCP监听表
- ▶ IGMP Snooping
- ▶ MAC 地址表

动态ARP检查表for Switch 1

开始从  , VLAN  , MAC address  和IP地址

端口	VLAN ID	MAC地址	IP 地址
无更多表项			

### 5)、IP Source Guard 列表

此页面显示当前 IP Source Guard 配置当前的列表：

- ▶ 系统
- ▶ 端口
- ▶ 网络安全
- ▶ LACP
  - 环路保护
  - 生成树
  - ARP 检测列表
  - IP Source Guard 列表
  - DHCP 监听表
- ▶ IGMP Snooping
- MAC 地址表
- ▶ VLANs

## 动态IP Source表for Switch 1

开始从  , VLAN  和IP地址  显示  每页显示条目

端口	VLAN ID	IP 地址	MAC地址
无更多表项			

## 6)、DHCP 监听表

此页面显示动态 IP 分配的信息，DHCP Snooping 功能模式被禁用。所有 DHCP 客户端获得来自 DHCP 服务器的动态 IP 地址将被列在该表中，除了本地的 VLAN 接口 IP 地址。在动态 DHCP Snooping 表项显示此页。

- ▶ 系统
- ▶ 端口
- ▶ 网络安全
- ▶ LACP
  - 环路保护
  - 生成树
  - ARP 检测列表
  - IP Source Guard 列表
  - DHCP 监听表
- ▶ IGMP Snooping
- MAC 地址表
- ▶ VLANs
- 堆叠

## 动态DHCP探测表

开始从MAC address  , VLAN  显示  每页显示条目

## 7)、IGMP Snooping

此页面显示 IGMP Snooping 的状态、组信息、IGMPv3 信息；

- ▶ 系统
- ▶ 端口
- ▶ 网络安全
- ▶ LACP
  - 环路保护
  - 生成树
  - ARP 检测列表
  - IP Source Guard 列表
  - DHCP 监听表
- ▶ IGMP Snooping
  - 状态
  - 组信息
  - IGMPv3 信息

## IGMP Snooping 状态 for Switch 1

统计

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted
---------	-----------------	--------------	----------------	---------------------

路由端口

端口	状态
1	-
2	-
3	-
4	-
5	-
6	-
7	-

## 8)、MAC 地址表

此页面显示连接在此端口上的 MAC 地址:

- 系统
- 端口
- 网络安全
- LACP
  - 环路保护
  - 生成树
- ARP 检测列表
- IP Source Guard 列表
- DHCP 监听表
- IGMP Snooping
- MAC 地址表
- VLANs
  - 堆叠

MAC地址表 for Switch 1

从VLAN ID  和MAC地址  起始显示,  每页的条目.

模式	VLAN	MAC 地址	端口成员																	
			CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
动态	1	00-01-C1-09-40-00		✓																
动态	1	00-01-C1-09-40-08		✓																
动态	1	00-01-EA-70-11-26		✓																
动态	1	00-07-E9-06-04-8D		✓																
动态	1	00-25-90-AA-6F-D2		✓																
动态	1	00-25-90-AA-72-CE		✓																
动态	1	00-3C-50-10-0A-30		✓																
动态	1	00-E0-4C-F8-90-C8		✓																
动态	1	00-E0-4C-F8-A6-66		✓																

## 9)、VLANs

此页面显示 VLANs 配置的显示信息; 包括 VLAN 成员、VLAN 端口状态:

- 系统
- 端口
- 网络安全
- LACP
  - 环路保护
  - 生成树
- ARP 检测列表
- IP Source Guard 列表
- DHCP 监听表
- IGMP Snooping
- MAC 地址表
- VLANs
  - VLAN 成员

VLAN 成员状态 Combined users for Switch 1

从VLAN ID  起始显示,  每页显示的条目. |<< >>|

VLAN ID	Port Members																									
	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	
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

- 系统
- 端口
- 网络安全
- LACP
  - 环路保护
  - 生成树
- ARP 检测列表
- IP Source Guard 列表
- DHCP 监听表
- IGMP Snooping
- MAC 地址表
- VLANs
  - VLAN 成员
  - VLAN 端口
  - 堆叠

VLAN 端口成员状态 Combined users for Switch 1

端口	端口类型	输入过滤	帧类型	Port VLAN ID	发送帧标记模式	UVID	冲突
1	C-Port	✓	All	1	Untag All		No
2	C-Port	✓	All	1	Untag All		No
3	C-Port	✓	All	1	Untag All		No
4	C-Port	✓	All	1	Untag All		No
5	C-Port	✓	All	1	Untag All		No
6	C-Port	✓	All	1	Untag All		No
7	C-Port	✓	All	1	Untag All		No
8	C-Port	✓	All	1	Untag All		No
9	C-Port	✓	All	1	Untag All		No
10	C-Port	✓	All	1	Untag All		No
11	C-Port	✓	All	1	Untag All		No
12	C-Port	✓	All	1	Untag All		No
13	C-Port	✓	All	1	Untag All		No
14	C-Port	✓	All	1	Untag All		No
15	C-Port	✓	All	1	Untag All		No
16	C-Port	✓	All	1	Untag All		No

## 10)、堆叠

此页面显示堆叠功能配置信息：包括堆叠拓扑、堆叠列表、主转发表；

Switch 1

- ▶ 系统
- ▼ 端口
  - 状态
  - 端口统计
  - 详细统计
- ▶ 网络安全
- ▶ LACP
  - 环路保护
- ▶ 生成树
  - ARP检测列表
  - IP Source Guard列表
  - DHCP监听表
- ▶ IGMP Snooping
- MAC 地址表
- ▶ VLANs
- 堆叠

### 堆叠拓扑

状态	开启堆叠
拓扑	Standalone
成员数	1
最后拓扑改变	1970-01-01T08:00:01+08:00
主Switch	00-55-44-33-22-11
最后拓扑改变	1970-01-01T08:00:01+08:00

### 堆叠列表

堆叠成员	Switch ID	结果	
		名字	版本
00-55-44-33-22-11	1	SMBStaX Switch	SMBStaX (stackable) 2013-12-16T10:47:38

### 主转发表

堆叠成员	Switch ID	端口	Distance		Forwarding	
			Port 25	Port 26	Port 25	Port 26
00-55-44-33-22-11	1	1-24,27-28	0	0	Local	Local

## 四、系统诊断

### 1、PING

显示 ICMP Ping 显示页面；

IP 址：输入要 ping 的 IP 地址。格式为 0.0.0.0

Ping 长度：ICMP 数据包的大小，值的范围从 2 个字节到 1452 个字节。

Ping 数：Ping ICMP 数据包的计数。值的范围从 1 到 60 。

Ping 间隔：Ping ICMP 数据包的间隔时间。值的范围 0 到 30 秒。

- Ping
- VeriPHY

### ICMP Ping

IP 地址	<input type="text" value="0.0.0.0"/>
Ping 长度	<input type="text" value="56"/>
Ping 数	<input type="text" value="5"/>
Ping 间隔	<input type="text" value="1"/>

## 2、VeriPHY

显示 VeriPHY Cable 诊断页面。通过端口选择；点击开始。便能检测相应的 Cable 状态：

- Ping
- VeriPHY

VeriPHY Cable诊断for Switch 1

端口

All

Cable 状态								
端口	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--
7	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--
9	--	--	--	--	--	--	--	--
10	--	--	--	--	--	--	--	--
11	--	--	--	--	--	--	--	--
12	--	--	--	--	--	--	--	--

## 五、系统维护

### 1、重新启动设备

当修改系统 MAC 地址等需要重启的设置后，建议重新启动设备来使设置生效。

- 重新启动设备
- 出厂默认值
- 软件上传
- 配置保存
- 配置下载
- 配置上传
- 配置激活
- 配置删除

重新启动设备

你是否需要重新启动设备？

### 2、出厂默认值

当需要将交换机配置还原到最初的系统默认值时，可选择恢复出厂配置功能。恢复以后设备管理 IP 地址信息、堆叠保存目前用户配置的不变，其他信息均会恢复为默认值，如登录账号密码恢复为：admin/admin、所有端口汇聚配置被清空等，所以在恢复出厂配置前请做好数据的记录工作。

- 重新启动设备
- 出厂默认值
- 软件上传
- 配置保存
- 配置下载
- 配置上传
- 配置激活
- 配置删除

出厂默认值

你是否要恢复出厂默认值？

## 3、软件上传

通过软件上传，点击浏览将最新的软件上传到设备中，达到软件升级。重启后生效。

- 重新启动设备
- 出厂默认值
- 软件上传
- 配置保存
- 配置下载
- 配置上传
- 配置激活
- 配置删除

### 软件上传

浏览...

## 4、配置保存

显示保存配置界面，通过该页面点击“配置保存”按钮，把当前配置保存到启动配置文件中，这样设备重启后配置文件才不会丢失。

- 重新启动设备
- 出厂默认值
- 软件上传
- 配置保存
- 配置下载
- 配置上传
- 配置激活
- 配置删除

### 保存当前配置到启动配置

请注意: 生成该配置文件需要耗费的,具体时间取决于配置

## 5、配置下载

此页面中有三种配置下载分别为：

running-config:运行配置；表示该交换机上的当前活动配置一个虚拟文件。

Default-config:启动配置；交换机的启动配置，在引导时读取。

Startup-config:默认配置；一个只读与供应商特定的配置文件。当系统恢复到默认设置该文件被读取。它也可以存储其它两个文件，并将其应用到运行配置，从而切换配置。

- 重新启动设备
- 出厂默认值
- 软件上传
- 配置保存
- 配置下载
- 配置上传
- 配置激活
- 配置删除

### 下载配置

选择需要下载的文件.

请注意: 正在配置的文件下载可能需要点准备时间.

文件名
<input type="radio"/> running-config
<input type="radio"/> default-config
<input type="radio"/> startup-config

## 6、配置上传

它可以从 Web 浏览器上传文件到交换机上的所有文件，除了默认的配置，它是只读的。

选择要上传，选择目标上的目标文件的文件，然后单击。

如果目标运行配置，该文件将被应用到交换机的配置。**这可以通过两种方式来完成：**

**替换模式：**当前配置完全与上传文件中的配置更换。

**合并模式：**上传的文件合并到运行配置。

如果文件系统已满（即包含上述三个系统文件以及其他两个文件），它是不可能建立新的文件，但现有的文件必须被覆盖或删除的另一个。

- 重新启动设备
- 出厂默认值
- 软件上传
- 配置保存
- 配置下载
- 配置上传
- 配置激活
- 配置删除

### 上传配置

选择配置文件

浏览...

目标文件

文件名	参数
<input type="radio"/> running-config	<input checked="" type="radio"/> 替换 <input type="radio"/> 合并
<input type="radio"/> startup-config	
<input type="radio"/> Create new file	<input type="text"/>

配置上传

## 7、配置激活

它可以激活任何现有交换机上的配置文件，除了运行配置代表了当前活动的配置。

选择文件来激活，然后按一下。这将启动与所选文件的完全替换现有的配置过程。

**注意：**激活的配置文件不会自动保存到启动配置文件中；需到配置保存里保存；在下次启动时才会加载当前配置。

- 重新启动设备
- 出厂默认值
- 软件上传
- 配置保存
- 配置下载
- 配置上传
- 配置激活
- 配置删除

### 激活配置

选择需要激活的配置文件。之前的配置被替换的话，有可能导致断开管理连接。

请注意：激活的配置文件不会自动的保存到启动配置文件中。

文件名

default-config

startup-config

配置激活

## 8、配置删除

它可以删除任何存储在闪存中的可写文件，包括启动配置的。如果这样做了，并重新启动交换机确保事先保存操作，重启后才能加载默认配置。

- 重新启动设备
- 出厂默认值
- 软件上传
- 配置保存
- 配置下载
- 配置上传
- 配置激活
- 配置删除

### 删除配置文件

选择待删除的配置文件。

文件名
<input type="radio"/> startup-config

配置文件删除
--------

## 六、硬恢复出厂设置

端口 1 与端口 24 对接。断电重启设备，当设备 SYS 闪烁，表示设备系统启动完成；观察端口 1 与端口 24 产生环路，快速闪，即表示恢复出厂设置；拔掉端口 1 与端口 24 的对接线。即可用默认 IP 进入 WEB 页面。