

MERCURY[®]

用户手册

全千兆智能网管交换机

REV1.0.2

1910060222

声明

Copyright © 2019 深圳市美科星通信技术有限公司

版权所有，保留所有权利

未经深圳市美科星通信技术有限公司明确书面许可，任何单位或个人不得擅自仿制、复制、誊抄或转译本手册部分或全部内容，且不得以营利为目的进行任何方式（电子、影印、录制等）的传播。

MERCURY®为深圳市美科星通信技术有限公司注册商标。本手册提及的所有商标，由各自所有人拥有。

本手册所提到的产品规格和资讯仅供参考，如有内容更新，恕不另行通知。除非有特殊约定，本手册仅作为使用指导，所作陈述均不构成任何形式的担保。

目录

第 1 章	用户手册简介	1
1.1	目标读者.....	1
1.2	本书约定.....	1
第 2 章	登录 Web 界面.....	2
2.1	登录准备.....	2
2.2	登录步骤.....	2
第 3 章	系统管理.....	4
3.1	系统信息.....	4
3.2	IP 设置	5
3.3	用户设置.....	6
3.4	系统工具.....	7
3.4.1	备份与还原	7
3.4.2	系统重启	8
3.4.3	系统恢复.....	8
3.4.4	系统升级.....	9
第 4 章	二层交换.....	10
4.1	端口管理.....	10
4.2	IGMP 侦听	11
4.3	汇聚管理.....	12
4.4	DHCP 侦听.....	14
第 5 章	监控.....	19
5.1	端口统计.....	19
5.2	端口镜像.....	20
5.3	线缆检测.....	21
5.4	环回检测.....	22
第 6 章	VLAN.....	23
6.1	MTU VLAN	23

6.2	端口 VLAN.....	24
6.3	802.1Q VLAN.....	25
6.4	802.1Q PVID 设置	26
第 7 章	服务质量.....	27
7.1	QoS 配置.....	27
7.2	带宽控制.....	29
7.3	风暴抑制.....	29
第 8 章	使用 Utility 管理软件	31
8.1	安装管理软件.....	31
8.2	使用管理软件.....	32
附录 A	常见问题.....	34

第1章 用户手册简介

本手册详细介绍登录Web管理交换机配置各项功能的方法，以及使用Utility管理软件的方法。请在操作前仔细阅读本手册。

1.1 目标读者

本手册的目标读者为熟悉网络基础知识、了解网络术语的技术人员。

1.2 本书约定

在本手册中，

- 所提到的“交换机”、“本产品”等名词，如无特别说明，系指全千兆智能网管交换机。
- 全文如无特殊说明，Web界面以SG116D Pro机型为例。
- 用 >> 符号表示配置界面的进入顺序。默认为**一级菜单 >> 二级菜单 >> 三级菜单**，其中，部分功能无二级菜单。
- 正文中出现的<>尖括号标记文字，表示Web界面的按钮名称，如<确定>。
- 正文中出现的“ ”双引号标记文字，表示Web界面出现的除按钮外名词，如“系统升级”界面。

本手册中使用的特殊图标说明如下：

图标	含义
 注意：	该图标提醒您对设备的某些功能设置引起注意，如果设置错误可能导致数据丢失，设备损坏等不良后果。
 说明：	该图标表示此部分内容是对相应设置、步骤的补充说明。

第2章 登录Web界面

2.1 登录准备

第一次登录时，需要确认以下几点：

1. 交换机已正常加电启动，任一端口已与管理主机相连。
2. 管理主机已至少安装一种以下浏览器：IE 8.0或以上版本，最新版本的FireFox、Chrome和Safari浏览器。
3. 管理主机IP地址已设为与交换机端口同一网段，即192.168.0.X（X为2至254之间的任意整数），子网掩码为255.255.255.0。
4. 为保证能更好地体验Web界面显示效果，建议将显示器的分辨率调整到1024×768或以上像素。

2.2 登录步骤

1. 打开IE浏览器，在地址栏中输入交换机默认管理地址<http://192.168.0.1>登录交换机的Web管理界面。



2. 交换机登录页面如下图所示，在此页面输入交换机管理帐号的用户名和密码，出厂默认值均为admin。

A screenshot of the Mercury web management login page. At the top, there is a dark grey header bar with the word "MERCURY" in white, bold, sans-serif capital letters. Below the header, the page has a light grey background. In the center, there are two text labels: "用户名:" (Username) and "密码:" (Password), each followed by a white rectangular input field with a thin blue border. Below these input fields, there are two buttons: "登陆" (Login) and "清除" (Clear), both with a light blue gradient and a thin blue border.

图 2-1 登录界面

3. 成功登录后将看到交换机的Web界面首页，如下图所示。



图 2-2 交换机首页界面

第3章 系统管理

3.1 系统信息

可以在此查看设备的系统信息，以及设置设备描述。

进入界面：系统管理 >> 系统信息

系统信息

设备描述：	SG116D Pro
MAC地址：	00:0A:EB:66:68:15
IP地址：	192.168.0.1
子网掩码：	255.255.255.0
默认网关：	0.0.0.0
软件版本：	1.0.0 Build 20180322 Rel.36865(Beta)
硬件版本：	SG116D Pro 1.0

设备描述：

SG116D Pro

应用

注意：
设备描述长度不能超过32个字符。

图 3-1 系统信息界面

界面项说明：

- 设备描述

显示设备的描述信息。

可以在下方“设备描述”框中输入自定义的设备描述信息，点击<应用>按键保存设置。自定义的设备描述长度不能超过32个字符。
- MAC地址

显示设备的MAC地址。
- IP地址

显示设备的IP地址。
- 子网掩码

显示设备的子网掩码。
- 默认网关

显示设备的默认网关。
- 软件版本

显示设备的软件版本。
- 硬件版本

显示设备的硬件版本。

3.2 IP设置

网络中每一台设备拥有一个独特的 IP 地址，可以通过这个 IP 地址登录管理界面操作交换机。

进入界面：系统管理 >> IP 设置

IP设置

DHCP设置：	禁用 ▼
IP地址：	192.168.0.1
子网掩码：	255.255.255.0
默认网关：	0.0.0.0

应用

帮助

图 3-2 IP设置界面

界面项说明：

DHCP设置	选择开启或禁用DHCP功能。 - 禁用：选择禁用，需手动输入IP地址、子网掩码和默认网关。 - 启用：选择启用，交换机会从DHCP服务器获取网络参数。
IP地址	设置设备的IP地址。
子网掩码	设置设备的子网掩码。
默认网关	设置设备的默认网关地址。

3.3 用户设置

可以在此修改登录时使用的用户名和密码。

进入界面：系统管理 >> 用户设置

用户设置

用户名：	admin
旧密码：	
新密码：	
确认密码：	

应用

帮助

注意：

用户名和新密码长度不能大于16个字符，且只能使用数字、英文字母和下划线。

图 3-3 用户设置界面

界面项说明：

用户名	设置登录交换机的用户名。用户名长度不能大于16个字符，且只能使用数字、英文字母和下划线。
旧密码	本次登录交换机使用的密码。
新密码	重新设置登录交换机的密码。新密码长度不能大于16个字符，且只能使用数字、英文字母和下划线。
确认密码	再次输入新密码。

3.4 系统工具

3.4.1 备份与还原

可以在此保存当前的配置信息，建议在修改配置及升级软件前备份当前配置信息。

进入界面：系统管理 >> 系统工具 >> 备份与还原

系统配置备份

点击配置备份按钮保存当前配置。
建议备份前保存当前配置。

配置备份

帮助

系统配置还原

选择一个备份配置文件然后点击恢复配置按钮，紧接着
你可以恢复交换机到它之前的配置。

配置文件：

浏览...

配置还原

帮助

注意：

- 1: 备份或还原配置需要花费几分钟时间，在此期间请不要进行其他操作。
- 2: 备份或还原配置过程中请不要断电，否则可能导致机器损坏。
- 3: 还原配置后，当前配置将会丢失。错误的配置可能导致交换机无法管理。

图 3-4 备份与还原界面

界面项说明：

➤ 系统配置备份

单击<配置备份>按键，交换机会将目前所有已保存配置导出为文件。建议在修改配置或升级软件前备份当前的配置信息。

➤ 系统配置还原

单击<浏览>按键，选择已备份的配置文件，然后点击<配置还原>按键，将交换机恢复到以前备份的配置状态。



注意：

- 备份或还原配置需要花费几分钟时间，在此期间请不要进行其他操作。
- 备份或还原配置过程中请不要断电，否则可能导致机器损坏。
- 还原配置后，当前配置将会丢失。错误的配置可能导致交换机无法管理。

3.4.2 系统重启

可以在此重启交换机。

进入界面：系统管理 >> 系统工具 >> 系统重启

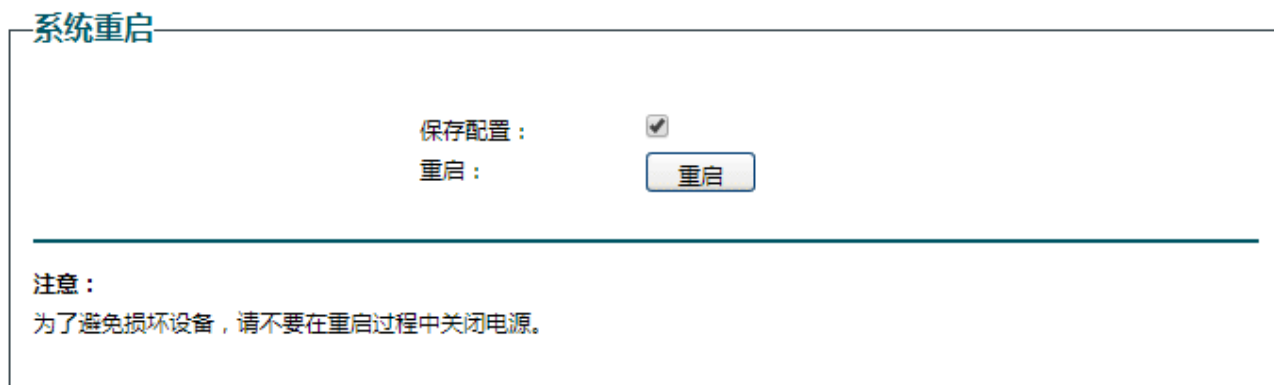


图 3-5 系统重启界面

单击<重启>按键，交换机将会重新启动。若勾选“保存配置”，则重新启动不会丢失已保存的配置。在重启的过程中，网络连接将会暂时中断。

 **注意：**
交换机重启过程中请保证电源稳定，避免强行断电。

3.4.3 系统恢复

可以在此将交换机的所有配置恢复到出厂时的默认状态。

进入界面：系统管理 >> 系统工具 >> 系统恢复

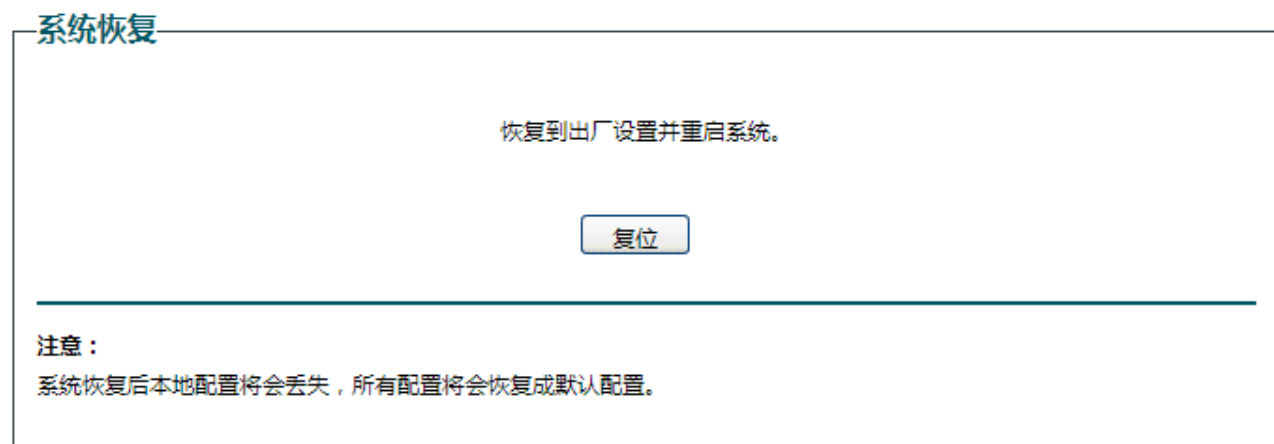


图 3-6 系统恢复界面

点击<复位>按键，交换机将会恢复所有设置的默认值。建议在网络配置错误、组网环境变更等情况时使用此功能。恢复出厂配置后，当前的配置信息将会丢失。如果不希望丢失当前配置，请先进行配置备份，再进行此操作。交换机出厂默认管理IP是192.168.0.1，默认用户名和密码均为admin。

3.4.4 系统升级

可以在此将交换机的软件升级到最新版本。

进入界面：系统管理 >> 系统工具 >> 系统升级

系统升级

通过升级交换机的软件，您将获得新的功能。

软件文件：

软件版本： 1.0.0 Build 20180322 Rel.36865(Beta)

硬件版本： SG116D Pro 1.0

注意：

- 1、为了避免损坏设备，请不要在升级过程中关闭电源。
- 2、建议在升级之前保存配置。
- 3、升级完成后，交换机将自动重启。

图 3-7 系统升级界面

MERCURY官方网站（<http://www.mercurycom.com.cn>）会不定期更新交换机的软件升级文件，可将升级文件下载保存在本地。登录交换机后进入本界面，单击<浏览>按钮，选择保存路径下的升级文件，单击<升级>按钮，进行软件升级。



注意：

- 升级软件可能会丢失当前未保存的配置信息，请在升级前保存配置。
- 软件升级过程中，请不要将设备断电，不要对页面进行刷新。
- 软件升级成功后，设备将自动重启，此过程中请保持电源稳定，避免强行断电。

第4章 二层交换

4.1 端口管理

可以在此为各物理端口配置基本的参数。

进入界面：二层交换 >> 端口管理

端口配置

端口	状态	速率/双工	流控
端口 1			
端口 2			
端口 3	启用	自动	关闭
端口 4			
端口 5			

应用

帮助

端口	状态	速率/双工		流控	
		配置	实际	配置	实际
端口 1	启用	自动	断开	关闭	关闭
端口 2	启用	自动	断开	关闭	关闭
端口 3	启用	自动	断开	关闭	关闭
端口 4	启用	自动	1000M全双工	关闭	关闭
端口 5	启用	自动	断开	关闭	关闭
端口 6	启用	自动	断开	关闭	关闭
端口 7	启用	自动	断开	关闭	关闭
端口 8	启用	自动	断开	关闭	关闭
端口 9	启用	自动	断开	关闭	关闭
端口 10	启用	自动	断开	关闭	关闭
端口 11	启用	自动	断开	关闭	关闭
端口 12	启用	自动	断开	关闭	关闭
端口 13	启用	自动	断开	关闭	关闭
端口 14	启用	自动	断开	关闭	关闭
端口 15	启用	自动	断开	关闭	关闭
端口 16	启用	自动	断开	关闭	关闭

注意：
当一个端口速率/双工设置为自动/1000M全双工并且它的实际模式是1000M全双工/100M全双工/10M全双工时，流控功能就可以开启并生效。

图 4-1 端口管理界面

界面项说明：

端口	选择配置的端口，可多选。
状态	选择启用或禁用端口。若启用端口，则端口可以正常转发报文。
速率/双工	为端口选择速率和双工模式。和交换机连接的设备应该具有相同的速率和双工，当模式选择为自动时，速率和双工将由协商决定。
流控	选择启用或禁用流控功能。推荐启用流控功能，以控制调节各端口数据包转发的速率，避免出现拥塞。

4.2 IGMP侦听

网络中的主机通过发送 IGMP（Internet Group Management Protocol，互联网组管理协议）报文向临近的路由器申请加入（或离开）组播组，当上层路由设备将组播数据转发下来后，交换机负责将组播数据转发给主机。IGMP 侦听（IGMP Snooping）是组播约束机制，运行 IGMP 侦听的交换机通过侦听和分析主机与组播路由器之间交互的 IGMP 报文来管理和控制组播组，从而可以有效抑制组播数据在网络中扩散。

进入界面：二层交换 >> IGMP 侦听

IGMP侦听

IGMP侦听：

☒ 启用 ☐ 禁用

Report报文抑制：

☐ 启用 ☒ 禁用

应用

帮助

IP地址	VLAN ID	端口
------	---------	----

图 4-2 IGMP侦听界面

界面项说明：

IGMP侦听	选择启用或禁用IGMP侦听功能。
Report报文抑制	选择启用或禁用Report报文抑制功能。如果开启该功能，则特定组播组的第一个Report报文将发往路由器端口，接下来的Report报文将被抑制，不发往路由器端口。Report报文抑制功能有助于减少网络中IGMP数据包的流量。
IP地址	查看组播IP地址。
VLAN ID	查看组播组对应的VLAN ID。
端口	查看组播组转发端口列表。

4.3 汇聚管理

LAG（Link Aggregation Group，端口汇聚组）是将交换机的多个物理端口汇聚在一起形成一个逻辑端口，同一汇聚组内的多条链路可视为一条逻辑链路。端口汇聚可以实现流量在汇聚组中各个成员端口之间进行分担，以增加带宽。同时，同一汇聚组的各个成员端口之间彼此动态备份，提高了连接可靠性。

属于同一个汇聚组中的成员端口必须有一致的配置，这些配置主要包括 QoS、VLAN、端口属性等。具体说明如下：

- 开启 802.1Q VLAN、QoS 配置及端口配置（速率、流控）功能的端口，若属于汇聚组成员，则他们的配置需保持一致。
- 开启端口镜像及半双工的端口，不能加入汇聚组。

如果需要配置汇聚组，建议在本功能处优先配置汇聚组后，再去其它功能处配置汇聚组的其它功能。



说明

- LAG 带宽的计算：当使用四个全双工 1000Mbps 端口构成 LAG 时，由于每一个端口上行和下行各是 1000Mbps，所以每一个端口的带宽为 2000Mbps。它们使用 LAG 技术汇聚在一起可以形成的最大总带宽为 8000Mbps。
- LAG 的流量会根据选路算法均衡分配到各个成员端口中去。当 LAG 中的一个或几个端口连接断开的时候，这些端口的流量会转移到 LAG 中其它链接正常的端口中去，即具备链路冗余备份功能。

进入界面：二层交换 >> 汇聚管理

汇聚配置

汇聚组

转发端口

汇聚 1 ▾

端口 1 ▲

端口 2

端口 3

端口 4 ▼

应用

汇聚组	转发端口	选择
汇聚 1	----	☐
汇聚 2	----	☐
汇聚 3	----	☐
汇聚 4	----	☐
汇聚 5	----	☐
汇聚 6	----	☐
汇聚 7	----	☐
汇聚 8	----	☐

全选

删除

帮助

注意：

1、最多创建 8 汇聚组。

2、每个汇聚组最多有 4 个成员端口。

3、镜像端口不能被加入到汇聚组。

图 4-3 汇聚管理界面

界面项说明：

- 汇聚组

选择汇聚组。
- 转发端口

选择属于汇聚组的物理端口。

说明

- 最多可创建 8 个汇聚组，每个汇聚组最多可以有 4 个成员端口。
- 镜像端口不能被加入到汇聚组。

4.4 DHCP侦听

随着网络规模的不断扩大和网络复杂度的提高，经常出现计算机的数量超过可供分配的 IP 地址的情况。同时随着便携机及无线网络的广泛使用，计算机的位置也经常变化，相应的 IP 地址也必须经常更新，从而导致网络配置越来越复杂。DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是在 BOOTP 协议基础上进行了优化和扩展而产生的一种网络配置协议，并有效解决了上面这些问题。

➤ DHCP 工作原理

DHCP 采用“客户端/服务器”通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的 IP 地址等配置信息，以实现网络资源的动态配置。通常一台服务器可以为多台客户端分配 IP，如图 13-5 所示：

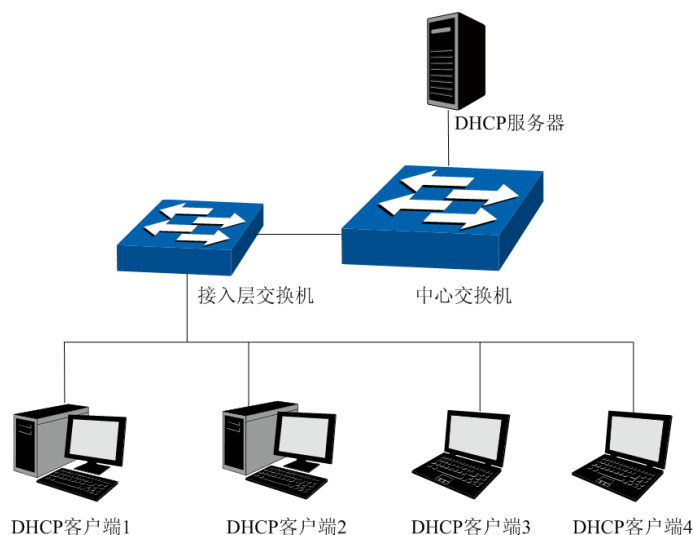


图 4-4 DHCP 网络典型应用

针对 DHCP 客户端的需求不同，DHCP 服务器提供三种 IP 地址分配策略：

- 1) 手工分配地址：由管理员为少数特定客户端（如 WWW 服务器等）静态绑定 IP 地址。通过 DHCP 将固定 IP 地址分配给客户端。
- 2) 自动分配地址：DHCP 服务器为客户端分配租期为无限长的 IP 地址。
- 3) 动态分配地址：DHCP 服务器为客户端分配具有一定有效期限的 IP 地址，当使用期限到期后，客户端需要重新申请地址。

绝大多数客户端均通过动态分配地址的方式获取 IP 地址，其获取 IP 地址的过程如下图所示：

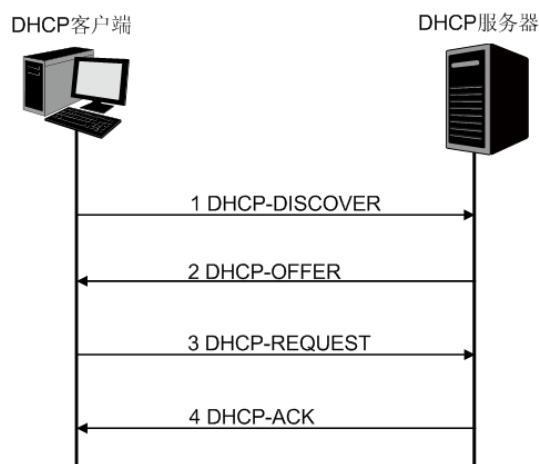


图 4-5 动态获取 IP 地址的过程

- 1) 发现阶段，客户端以广播方式发送 DHCP-DISCOVER 报文寻找 DHCP 服务器。
- 2) 提供阶段，DHCP 服务器接收到客户端发送的 DHCP-DISCOVER 报文后，根据 IP 地址分配的优先次序从地址池中选出一个 IP 地址，与其它参数一起通过 DHCP-OFFER 报文发送给客户端（发送方式根据客户端发送的 DHCP-DISCOVER 报文中的 flag 字段决定，具体请见 DHCP 报文格式的介绍）。
- 3) 选择阶段，如果有多台 DHCP 服务器向该客户端发来 DHCP-OFFER 报文，客户端只接受第一个收到的 DHCP-OFFER 报文，然后以广播方式发送 DHCP-REQUEST 报文，该报文中包含 DHCP 服务器在 DHCP-OFFER 报文中分配的 IP 地址。
- 4) 确认阶段，DHCP 服务器收到 DHCP 客户端发来的 DHCP-REQUEST 报文后，只有 DHCP 客户端选择的服务器会进行如下操作：如果确认地址分配给该客户端，则返回 DHCP-ACK 报文；否则将返回 DHCP-NAK 报文，表明地址不能分配给该客户端。

➤ Option 82

DHCP 报文格式基于 BOOTP 的报文格式，共有 8 种类型的报文，每种报文的格式相同。DHCP 和 BOOTP 消息的不同主要体现在选项（Option）字段，并利用 Option 字段来实现功能扩展。例如 DHCP 可以利用 Option 字段传递控制信息和网络配置参数，实现地址的动态分配，为客户端提供更加丰富的网络配置信息。更多 DHCP Option 选项的介绍，请参见 RFC 2132。

Option 82 选项记录了 DHCP 客户端的位置信息，交换机接收到 DHCP 客户端发送给 DHCP 服务器的请求报文后，在该报文中添加 Option 82，并转发给 DHCP 服务器。管理员可以从 Option 82 中获得 DHCP 客户端的位置信息，以便定位 DHCP 客户端，实现对客户端的安全和计费等控制。支持 Option 82 的服务器还可以根据该选项的信息制订 IP 地址和其它参数的分配策略，提供更加灵活的地址分配方案。

Option 82 最多可以包含 255 个子选项。若定义了 Option 82，则至少要定义一个子选项。目前本交换机支持两个子选项：Circuit ID（电路 ID 子选项）和 Remote ID（远程 ID 子选项）。由于 Option 82 的内容没有统一规定，不同厂商通常根据需要进行填充。目前本交换机对子选项的填充内容如下，电路 ID 子选项的填充内容是接收到 DHCP 客户端请求报文的端口所属 VLAN 的编号以及端口号，远程 ID 子选项的填充内容是接收到 DHCP 客户端请求报文的 DHCP Snooping 设备的 MAC 地址。

➤ DHCP 服务欺骗攻击

在 DHCP 工作过程中，通常服务器和客户端没有认证机制，如果网络上存在多台 DHCP 服务器，不仅会给网络造成混乱，也对网络安全造成很大威胁。这种网络中出现非法的 DHCP 服务器，通常分为两种情况：

- 1) 用户不小心配置的 DHCP 服务器，由此引起的网络混乱非常常见。
- 2) 黑客将正常的 DHCP 服务器中的 IP 地址耗尽，然后冒充合法的 DHCP 服务器，为客户端分配 IP 地址等配置参数。例如黑客利用冒充的 DHCP 服务器，为用户分配一个经过修改的 DNS 服务器地址，在用户毫无察觉的情况下被引导至预先配置好的假的金融网站或电子商务网站，骗取用户的帐户和密码，如图 13-7 所示。

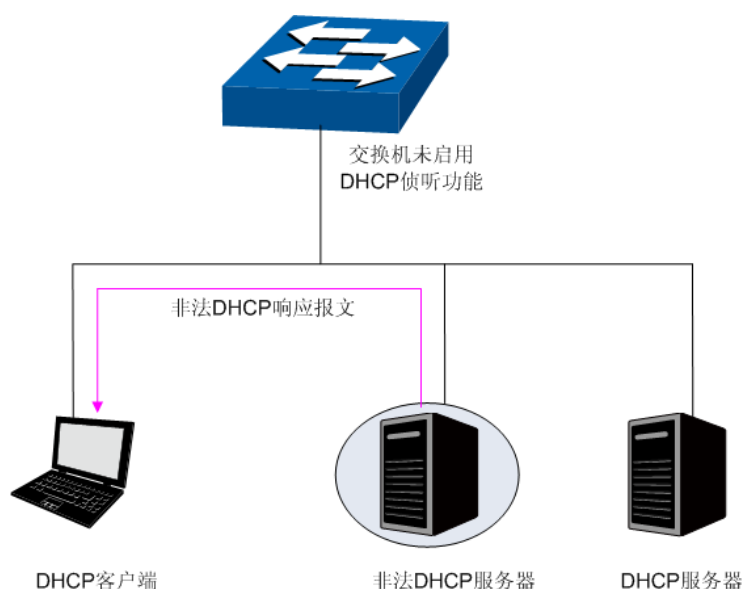


图 4-6 DHCP 服务欺骗攻击

DHCP 侦听是运行在交换机上的一种 DHCP 安全特性。通过设置 DHCP 服务器的连接端口为授信端口，只处理授信端口发来的 DHCP 响应报文；通过监听 DHCP 报文，记录用户从 DHCP 服务器获取局域网用户的四元信息，进行绑定后与 ARP 攻击防护配合使用；同时也可以过滤不可信任的 DHCP 信息，防止局域网中发生 DHCP 服务欺骗攻击，提高网络的安全性。

进入页面的方法：二层交换 >> DHCP 侦听

DHCP侦听

DHCP侦听：

启用

禁用

应用

端口配置

端口	信任	Option82	模式	电路ID自定义	电路ID子选项	远程ID自定义	远程ID子选项
端口 1							
端口 2							
端口 3							
端口 4							
端口 5							

应用

帮助

端口	信任	Option82	模式	电路ID自定义	电路ID子选项	远程ID自定义	远程ID子选项
端口1	禁用	禁用	保留	禁用		禁用	
端口2	禁用	禁用	保留	禁用		禁用	
端口3	禁用	禁用	保留	禁用		禁用	
端口4	禁用	禁用	保留	禁用		禁用	
端口5	禁用	禁用	保留	禁用		禁用	
端口6	禁用	禁用	保留	禁用		禁用	
端口7	禁用	禁用	保留	禁用		禁用	
端口8	禁用	禁用	保留	禁用		禁用	
端口9	禁用	禁用	保留	禁用		禁用	
端口10	禁用	禁用	保留	禁用		禁用	
端口11	禁用	禁用	保留	禁用		禁用	
端口12	禁用	禁用	保留	禁用		禁用	
端口13	禁用	禁用	保留	禁用		禁用	
端口14	禁用	禁用	保留	禁用		禁用	
端口15	禁用	禁用	保留	禁用		禁用	
端口16	禁用	禁用	保留	禁用		禁用	

图 4-7 DHCP 侦听全局配置

条目介绍：

DHCP 侦听配置

DHCP 侦听：选择是否启用 DHCP 侦听功能。

端口：显示交换机的端口号。

授信端口：选择是否配置端口为授信端口，只有授信端口才正常转发来自正常 DHCP 服务器端的消息，请将连接有 DHCP 服务器的端口设为授信端口。

Option 82 支持:	选择是否启用 Option 82 功能。
已有 Option 82 处理:	当客户端的 DHCP 请求报文已经有 Option 82 字段时，选择对此字段的操作。 ● 保留：保留数据包中的 Option 字段信息。 ● 替换：替换数据包中的 Option 字段信息，替换为交换机自定义的系统选项内容。 ● 丢弃：丢弃包含 Option 82 字段的数据包。
电路 ID 自定义:	选择是否开启电路 ID 自定义。如果关闭，则 ID 默认为收到报文的 VLAN 和端口字段。
电路 ID 子选项:	输入交换机自定义的 Option 82 选项中电路 ID 子选项的内容。支持使用%hostname,%macaddr,%port 来表示设备名，MAC 地址和端口号。
远程 ID 自定义:	选择交换机是否自定义 Option 82 选项内容。
远程 ID 子选项:	输入交换机自定义的 Option 82 选项中远程 ID 子选项的内容。支持使用%hostname,%macaddr,%port 来表示设备名，MAC 地址和端口号。

第5章 监控

5.1 端口统计

端口统计信息显示各个端口的流量信息，方便监控流量并分析网络异常。

进入界面：监控 >> 端口统计

端口统计						
端口	状态	双工模式	正常发包	失败发包	正常收包	失败收包
端口 1	启用	断开	0	0	0	0
端口 2	启用	断开	0	0	0	0
端口 3	启用	1000M全双工	225	0	3366	0
端口 4	启用	断开	0	0	0	0
端口 5	启用	断开	0	0	0	0
端口 6	启用	断开	0	0	0	0
端口 7	启用	断开	0	0	0	0
端口 8	启用	断开	0	0	0	0
端口 9	启用	断开	0	0	0	0
端口 10	启用	断开	0	0	0	0
端口 11	启用	断开	0	0	0	0
端口 12	启用	断开	0	0	0	0
端口 13	启用	断开	0	0	0	0
端口 14	启用	断开	0	0	0	0
端口 15	启用	断开	0	0	0	0
端口 16	启用	断开	0	0	0	0

刷新

清空

帮助

图 5-1 端口统计界面

界面项说明：

- 端口

显示端口号。
- 状态

显示端口状态。只有状态为启用时，端口才能正常转发数据包。
- 双工模式

显示端口双工模式。
- 正常发包

显示端口正常发包数。
- 失败发包

显示端口失败发包数。
- 正常收包

显示端口正常收包数。

失败收包 显示端口失败收包数。

5.2 端口镜像

端口镜像将一个端口的数据转发到一个镜像端口。通常，镜像端口和诊断设备相连来分析或者监控网络。

进入界面：监控 >> 端口镜像

镜像端口

端口镜像使能	镜像端口
禁用 ▼	

应用

被镜像端口

被镜像端口	入口	出口
端口 1 端口 2 端口 3 端口 4 端口 5		

应用

帮助

被镜像端口	入口	出口
端口1	禁用	禁用
端口2	禁用	禁用
端口3	禁用	禁用
端口4	禁用	禁用
端口5	禁用	禁用
端口6	禁用	禁用
端口7	禁用	禁用
端口8	禁用	禁用
端口9	禁用	禁用
端口10	禁用	禁用
端口11	禁用	禁用
端口12	禁用	禁用
端口13	禁用	禁用
端口14	禁用	禁用
端口15	禁用	禁用
端口16	禁用	禁用

图 5-2 端口镜像界面

界面项说明：

➤ 镜像端口

端口镜像使能 选择启用或禁用端口镜像功能。

镜像端口 只能选择一个端口做镜像端口。

➤ 被镜像端口

被镜像端口 被镜像端口可以为多个，但不包含当前的镜像端口。

入口 选择启用或者禁用入口功能。当入口功能启用，从被镜像端口进入的包将会被拷贝到镜像端口。

出口 选择启用或者禁用出口功能。当出口功能启用，从被镜像端口出去的包将会被拷贝到镜像端口。

5.3 线缆检测

当线缆连接到交换机端口时，线缆测试功能可以测试线缆连接状态，线缆长度和误差长度，方便定位和诊断网络故障点。

进入界面：监控 >> 线缆检测

线缆检测

选择	端口	检测结果	出错距离(m)
☐	端口 1	--	--
☐	端口 2	--	--
☐	端口 3	--	--
☐	端口 4	--	--
☐	端口 5	--	--
☐	端口 6	--	--
☐	端口 7	--	--
☐	端口 8	--	--
☐	端口 9	--	--
☐	端口 10	--	--
☐	端口 11	--	--
☐	端口 12	--	--
☐	端口 13	--	--
☐	端口 14	--	--
☐	端口 15	--	--
☐	端口 16	--	--

全选

应用

帮助

注意：
被禁用端口不能进行线缆检测。

图 5-3 线缆检测界面

界面项说明：

选择/端口	勾选需进行线缆检测的端口，可多选。
检测结果	检测端口连接的线缆的状态。可能显示的状态有：正常、短路、开路、阻抗。另外还可能出现线路不支持检测或检测失败的情况。 ■ 开路：线路中有断开现象，造成这种情况的原因一般是水晶头处线缆接触不良，可用线缆测试设备进行故障点定位。 ■ 短路：线路金属内芯互相接触，导致短路。 ■ 阻抗：网线质量问题。
出错距离	若线路为正常状态，显示该线缆的长度范围。若线路为短路、开路或阻抗状态，则显示该线缆的出错长度。



说明

- 对同一个端口前后两次诊断，请间隔 3 秒以上。
- 当电缆对端未连接时，诊断结果会较为准确。
- 这里的长度是指线缆绕对的长度，不是线缆表皮长度，线缆检测的长度可能存在误差。
- 检测结果仅供参考，特殊的情况也可能会检测错误或失败。

5.4 环回检测

环回保护功能被用来检测由特定端口创建的回环。

进入界面：监控 >> 环回检测

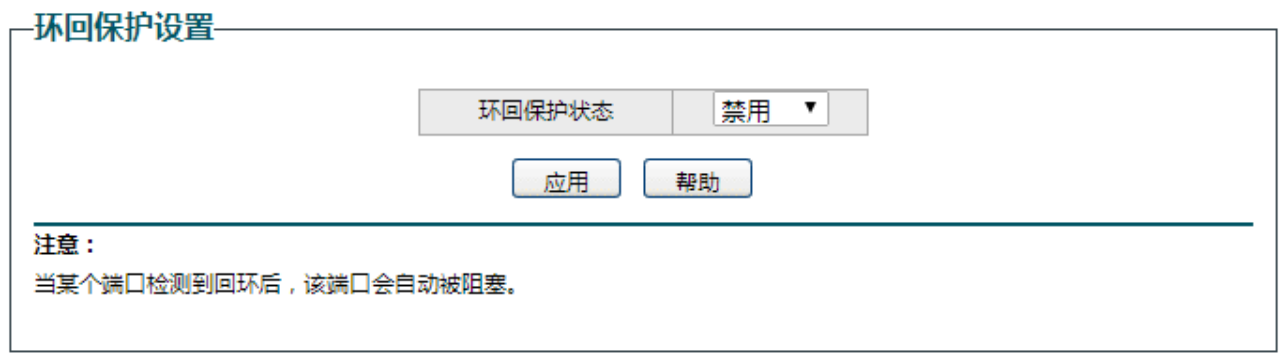


图 5-4 环回检测界面

选择启用“环回保护状态”，可开启环回保护功能。当某个端口检测到回环后，该端口会自动被阻塞。

第6章 VLAN

VLAN（Virtual Local Area Network，虚拟局域网）是一种将局域网设备从逻辑上划分成一个个网段，从而实现虚拟工作组的数据交换技术，这种技术通过在局域网数据帧上定义扩展字段，来对物理网络进行逻辑上的分割，从而限定局域网数据帧的转发范围，缩小广播域。VLAN 技术主要应用于交换机、路由器和交换机等网络设备中。

6.1 MTU VLAN

MTU VLAN（Multi-Tenant Unit VLAN）是将每个用户所占用的端口与上联端口（Uplink端口）划分为一个单独的VLAN。普通端口只能和预先设置的上联端口进行通信，相互之间无法通信，从而可保障网络的安全。

进入界面：VLAN >> MTU VLAN

MTU VLAN设置

MTU VLAN使能：☐ 启用 ☒ 禁用 应用

当前Uplink端口：	1
改变Uplink端口：	端口 1 ▼

应用 帮助

图 6-1 MTU VLAN界面

界面项说明：

- MTU VLAN使能 选择启用或禁用MTU VLAN功能。
- 当前Uplink端口 显示当前Uplink端口。
- 改变Uplink端口 重新选择Uplink端口。

6.2 端口VLAN

端口 VLAN 是基于端口划分 VLAN，可以把交换机的端口从逻辑上划分为多个 VLAN。

进入界面：VLAN >> 端口 VLAN

端口VLAN设置

端口VLAN使能：☒ 启用 ☐ 禁用 应用

VLAN	(2-16)							
端口	1	2	3	4	5	6	7	8
成员	☐	☐	☐	☐	☐	☐	☐	☐
端口	9	10	11	12	13	14	15	16
成员	☐	☐	☐	☐	☐	☐	☐	☐

应用 帮助

VLAN	VLAN成员端口	删除
1	1-16	☐

全选 删除

图 6-2 端口VLAN界面

界面项说明：

端口VLAN使能 选择启用或禁用端口VLAN功能。

VLAN 设置VLAN ID，取值范围2-16。

端口/成员 选择属于该VLAN的成员端口。

6.3 802.1Q VLAN

802.1Q VLAN 是基于 IEEE802.1Q 协议对 VLAN 进行分类的方法。VLAN 由 VLAN ID（VID）区分，所有到达端口的 Untagged 数据包都会被标记端口 PVID 的 Tag。

进入界面：VLAN >> 802.1Q VLAN

802.1Q VLAN使能：☐ 启用 ☒ 禁用

应用

VLAN	(1-4094)	VLAN描述	
端口	Untagged端口	Tagged端口	非成员
全选	☐	☐	☐
端口 1	☐	☐	☒
端口 2	☐	☐	☒
端口 3	☐	☐	☒
端口 4	☐	☐	☒
端口 5	☐	☐	☒
端口 6	☐	☐	☒
端口 7	☐	☐	☒
端口 8	☐	☐	☒
端口 9	☐	☐	☒
端口 10	☐	☐	☒
端口 11	☐	☐	☒
端口 12	☐	☐	☒
端口 13	☐	☐	☒
端口 14	☐	☐	☒
端口 15	☐	☐	☒
端口 16	☐	☐	☒

添加/编辑

帮助

VLAN	VLAN描述	成员端口	Tagged端口	Untagged端口	删除
------	--------	------	----------	------------	----

全选

删除

图 6-3 802.1Q VLAN 界面

界面项说明：

- 802.1Q VLAN使能

选择启用或禁用802.1Q VLAN功能。
- VLAN

设置VLAN ID，取值范围1-4094。
- VLAN描述

设置VLAN的描述信息，以方便管理和查找。
- Untagged端口

若选择为Untagged端口，则输出的数据帧不带tag信息。
- Tagged端口

若选择为Tagged端口，则输出的数据帧带tag信息。
- 非成员

选择后，表示该端口不属于VLAN的成员端口。

6.4 802.1Q PVID设置

PVID（端口 VLAN ID）是端口缺省 VID。当端口接收到一个 Untagged 包，将给这个包添加一个带有端口 PVID 的 VLAN Tag，并转发该数据包。

进入界面：VLAN >> 802.1Q PVID 设置

802.1Q VLAN PVID设置

选择	端口	PVID
☐		
☐	端口1	1
☐	端口2	1
☐	端口3	1
☐	端口4	1
☐	端口5	1
☐	端口6	1
☐	端口7	1
☐	端口8	1
☐	端口9	1
☐	端口10	1
☐	端口11	1
☐	端口12	1
☐	端口13	1
☐	端口14	1
☐	端口15	1
☐	端口16	1

应用

帮助

注意：

1、缺省情况下所有端口的PVID都是1。

2、当802.1Q VLAN被禁用后，所有端口的PVID会被恢复到1。

图 6-4 802.1Q PVID设置界面

界面项说明：

选择/端口 选择需要设置PVID的端口。

PVID 设置端口的PVID。

 **说明**

- 缺省情况下所有端口的 PVID 都是 1。
- 当 802.1Q VLAN 被禁用后，所有端口的 PVID 会被恢复到 1。

第7章 服务质量

服务质量模块主要用于流量控制管理和优先级配置，针对各种网络应用的不同需求，为其提供不同的服务质量，对带宽资源进行最优配置，从而提供更高质量的网络服务体验。

7.1 QoS配置

QoS（Quality of Service即服务质量）功能用于优化网络性能，提供更好的网络服务体验。交换机基于端口、802.1P和DSCP实现三种优先级模式。

进入界面：服务质量 >> QoS 配置

全局配置

QoS模式：

☒ 基于端口

☐ 基于802.1P

☐ 基于DSCP

应用

帮助

基于端口优先级设置

选择	端口	优先级队列
☐		1 (低) ▼
☐	端口 1	1(低)
☐	端口 2	1(低)
☐	端口 3	1(低)
☐	端口 4	1(低)
☐	端口 5	1(低)
☐	端口 6	1(低)
☐	端口 7	1(低)
☐	端口 8	1(低)
☐	端口 9	1(低)
☐	端口 10	1(低)
☐	端口 11	1(低)
☐	端口 12	1(低)
☐	端口 13	1(低)
☐	端口 14	1(低)
☐	端口 15	1(低)
☐	端口 16	1(低)

应用

注意：

1、最低优先级（背景数据）

2、普通优先级（关键业务数据，电子邮件，互联网等）

3、中等优先级（流多媒体数据等）

4、最高优先级（语音会话，视频，低延迟数据）

图 7-1 QoS配置界面

界面项说明：

➤ 全局配置

本交换机共有基于端口的优先级、IEEE 802.1P 优先级和 DSCP 优先级三种模式。其中基于端口的优先级是默认被启用的，其它两种优先级模式可供选择。

- 基于端口：基于入端口这些包被映射到 4 个不同的优先级级别。
- 基于 802.1P：802.1P 给 802.1Q Tag 的优先级字段一个推荐的定义。Tagged 包被映射到 4 个优先级（最低=1,2 / 普通=0,3 / 中等=4,5 / 高=6,7）。
- 基于 DSCP：DSCP 给了 IP DSCP 字段一个推荐的定义。IP 数据包根据 DSCP 值映射到 4 个优先级（最低=0-15 / 普通=16-31 / 中等=32-47 / 高=48-63）。

➤ 基于端口优先级设置

选择/端口 勾选端口配置端口优先级，可多选。

优先级队列 选择端口的优先级。

7.2 带宽控制

带宽控制是通过设定端口可用带宽，来控制端口的输入/输出数据传输速率，从而合理地分配和利用网络带宽。

进入界面：服务质量 >> 带宽控制

带宽控制

选择	端口	入口限速(Kbps)	出口限速(Kbps)
☐		 (0-1000000)	 (0-1000000)
☐	端口 1	无限制	无限制
☐	端口 2	无限制	无限制
☐	端口 3	无限制	无限制
☐	端口 4	无限制	无限制
☐	端口 5	无限制	无限制
☐	端口 6	无限制	无限制
☐	端口 7	无限制	无限制
☐	端口 8	无限制	无限制
☐	端口 9	无限制	无限制
☐	端口 10	无限制	无限制
☐	端口 11	无限制	无限制
☐	端口 12	无限制	无限制
☐	端口 13	无限制	无限制
☐	端口 14	无限制	无限制
☐	端口 15	无限制	无限制
☐	端口 16	无限制	无限制

应用

帮助

图 7-2 带宽控制界面

界面项说明：

- 选择/端口

勾选端口配置端口带宽，可多选。
- 入口限速

设置入口限速。
- 出口限速

设置出口限速。

7.3 风暴抑制

广播风暴是指网络上的广播帧由于不断被转发导致数量急剧增加而影响正常的网络通讯，严重降低网络性能。广播风暴的判断标准为一个端口是否在短时间内连续收到许多个广播帧。风暴抑制是指用户可以

限制端口上允许接收的广播流量大小，当该类流量超过用户设置的阈值后，系统将丢弃超出流量限制的广播帧，防止广播风暴的发生，从而保证网络的正常运行。

本交换机可以对三种常见的广播帧（广播包、组播包、UL包）进行限制。

进入界面：服务质量 >> 风暴抑制

风暴抑制

选择	端口	状态	速率(Kbit/sec)	风暴类型
☐		禁用 ▼	 (1-1000000)	UL包 组播包 广播包
☐	端口 1	禁用	无限制	
☐	端口 2	禁用	无限制	
☐	端口 3	禁用	无限制	
☐	端口 4	禁用	无限制	
☐	端口 5	禁用	无限制	
☐	端口 6	禁用	无限制	
☐	端口 7	禁用	无限制	
☐	端口 8	禁用	无限制	
☐	端口 9	禁用	无限制	
☐	端口 10	禁用	无限制	
☐	端口 11	禁用	无限制	
☐	端口 12	禁用	无限制	
☐	端口 13	禁用	无限制	
☐	端口 14	禁用	无限制	
☐	端口 15	禁用	无限制	
☐	端口 16	禁用	无限制	

应用

帮助

图 7-3 风暴抑制界面

界面项说明：

- 选择/端口

勾选端口配置风暴抑制参数，可多选。
- 状态

选择启用或禁用风暴抑制功能。
- 速率

在端口上输入广播/组播/UL包的带宽，超过带宽的包流量将被丢弃。
- 风暴类型

选择端口的风暴抑制类型，可多选。

第8章 使用Utility管理软件

8.1 安装管理软件

1. 将光盘插入计算机的光盘驱动器。
2. 打开CD-ROM所在的驱动器，可以看到“水星智能网管交换机客户端应用程序”的安装程序目录，双击其中的“水星智能网管交换机客户端应用程序.exe”开始安装，会出现如下图所示的欢迎界面。

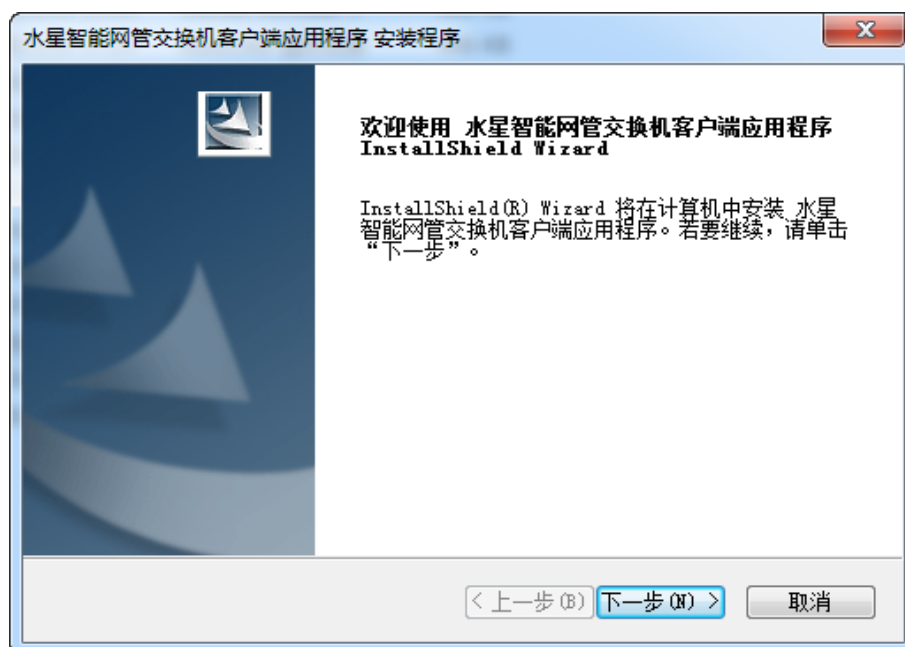


图 8-1 安装管理软件

3. 点击<下一步>按钮，可进行下一步操作，按照提示，经过几步操作，可完成软件安装，如下图所示。

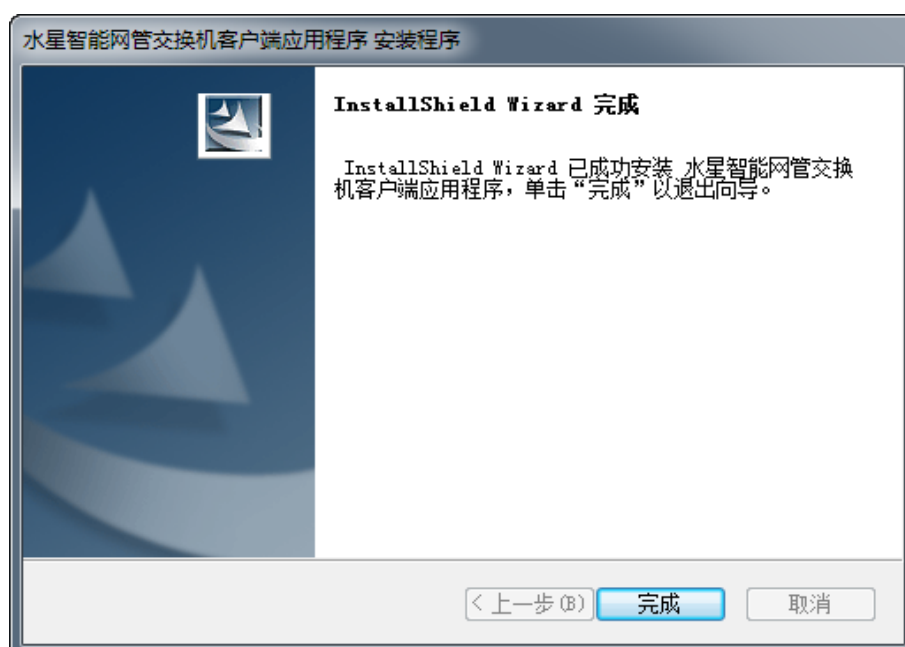


图 8-2 软件安装完成

8.2 使用管理软件

1. 双击桌面上的“水星智能网管交换机客户端应用程序.exe”快捷方式，将出现如下图所示交换机列表界面。



The screenshot shows the Mercury Network Management Software interface. At the top is the 'MERCURY' logo. Below it is a title bar for the '交换机列表' (Switch List) window. The main area contains a table with the following columns: '产品型号' (Product Model), '设备描述' (Device Description), 'MAC地址' (MAC Address), 'IP地址' (IP Address), '主机IP地址' (Host IP Address), 'IP设置' (IP Settings), and '登录' (Login). The first row of data shows 'SG116D Pro' for both product model and device description, with MAC address '00-0A-EB-66-68-46', IP address '192.168.0.1', and host IP address '192.168.0.100'. The 'IP设置' column has a gear icon, and the '登录' column has a user icon. Below the table are two buttons: '帮助' (Help) on the left and '刷新' (Refresh) on the right.

产品型号	设备描述	MAC地址	IP地址	主机IP地址	IP设置	登录
SG116D Pro	SG116D Pro	00-0A-EB-66-68-46	192.168.0.1	192.168.0.100	⚙️	👤

图 8-3 交换机列表

运行“水星智能网管交换机客户端应用程序”时，若没有正常连接计算机与交换机，则会出现如下图所示错误提示。

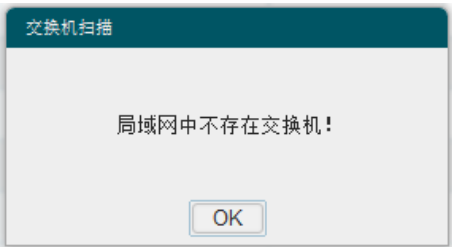


图 8-4 错误提示

2. 在如图 8-3所示界面的“交换机列表”中，双击对应的交换机条目或点击“登录”图标，可以打开如下图所示的登录界面，在此界面输入交换机管理账号的用户名和密码，出厂默认值均为admin。



The login interface for the Mercury SG116D Pro 1.0. It features the Mercury logo at the top. Below the logo are two input fields: the first for the username, which contains 'admin', and the second for the password, which contains six dots. A checkbox labeled '记住用户名和密码' (Remember username and password) is checked. At the bottom are two buttons: '登录' (Login) and '取消' (Cancel).

图 8-5 登录界面

3. 经过上述步骤即可成功进入交换机管理软件界面，如下图所示。点击主页左侧的主菜单栏即可进行相应功能的配置。



The management software interface for the Mercury SG116D Pro 1.0. The top bar shows the Mercury logo and the device name 'SG116D Pro 1.0'. Below this is a navigation bar with tabs: '系统管理' (System Management), '二层交换' (Layer 2 Switching), '监控' (Monitoring), 'VLAN', '服务质量' (Quality of Service), and '帮助' (Help). The '系统管理' tab is selected. On the left is a sidebar with a '系统信息' (System Information) section containing links for 'IP设置' (IP Settings), '用户设置' (User Settings), '备份与还原' (Backup and Restore), '系统重启' (System Restart), '系统恢复' (System Recovery), and '系统升级' (System Upgrade). The main content area shows the '系统信息' (System Information) page. It contains a table with the following information:

设备描述:	SG116D Pro
MAC地址:	00-0A-EB-66-68-46
IP地址:	192.168.0.1
子网掩码:	255.255.255.0
默认网关:	0.0.0.0
软件版本:	1.0.0 Build 20180412 Rel.52152
硬件版本:	SG116D Pro 1.0

Below the table is a form for editing the '设备描述' (Device Description) field, which currently contains 'SG116D Pro'. There is an '应用' (Apply) button next to the field. A note at the bottom states: '注意：设备描述长度不能超过32个字符。' (Note: Device description length cannot exceed 32 characters.)

图 8-6 管理软件界面

说明

使用管理软件配置交换机功能的方法与登录 Web 界面管理交换机方法类似，不单独介绍。

附录A 常见问题

问题1：无法登录交换机Web管理界面该如何处理？

1. 如果第一次使用此交换机，请参考以下步骤：
 - 1) 确认网线已正常连接到了交换机的LAN口，对应的指示灯闪烁或者常亮。
 - 2) 访问设置界面前，建议手动设置 IP 地址，将计算机的 IP 地址与交换机地址设置为同一网段。
 - 3) 使用ping命令检测计算机与交换机之间的连通性。
 - 4) 若上述提示仍不能帮助您登录到交换机管理界面，请将交换机恢复为出厂配置。
2. 如果之前可以正常登录，现在不能登录，则有可能是他人修改了交换机的配置导致的，建议恢复出厂配置，修改交换机管理账号的用户名和密码，做好保密措施。
3. 如果恢复出厂配置后仍然无法登录或开始一段时间能登录，但过一段时间后又不能登录，则可能是遭受了ARP欺骗，建议查找欺骗源、查杀病毒或将其隔离。
4. 请检查是否设置了IE代理，如果设置了IE代理，请先将代理取消。

问题2：忘记交换机用户名和密码怎么办？如何恢复出厂配置？

忘记用户名密码时可以将交换机通过Reset键恢复至出厂配置。需要注意的是：恢复出厂配置时交换机原有配置信息将丢失。

恢复出厂配置操作方法：通电状态下长按Reset键，等待2~5秒后，见到除Power指示灯外所有指示灯熄灭，松开按键，交换机将自动恢复出厂设置并重启。交换机出厂默认管理IP是192.168.0.1，默认用户名和密码均为admin。