NSW1924F
用户手册

V1.0

2009-09-16

商标、版权声明

本文档提供的资料，如有变更，恕不另行通知。**磊科**®是磊科网络有限公司的注册商标。本文档提及的其他所有商标和注册商标，由各自的所有人拥有。

http://www.netcoretec.com

认证

通过 FCC 认证

包装内容

包装盒里面应该有以下东西：

- Ø 一台 NSW1924F
- Ø 一张 CD
- Ø 一本安装指南
- Ø 一根电缆线
- Ø 一根电源线
- Ø 一副耳片

请确认包装盒里面有上述所有东西，如果有任何一个配件损坏或者丢失，请与你的经销商联系。

目录

1. 简介

欢迎选用 NSW1924F

1.1. 产品概述

NSW1924F 有 16 个千兆 SFP 光模块接口，4 个千兆光铜 combo 和 4 个千兆铜缆口，它是磊科公司推出的具有高性能、多用途、高安全性的网管型光纤交换机。本交换机支持 IEEE802.3 10BASE-T/802.3u 100BASE-TX、IEEE 802.3ab 1000Base-T IEEE 802.3Z 千兆以太网标准，支持自动协商功能，支持 MAC 地址绑定、MAC 地址过滤、MAC 地址学习、MAC 地址老化，支持 web 页面设置以及固件升级等功能。NSW1924F 具有全智能自动绑定、全面安全保护、网刻分流、无盘优化、联动网管，管理便捷等优点，选用这一款功能强大的磊科 NSW1924F 是您明智的选择！

1.2. 主要特性

- Ø 支持 MAC 地址绑定
- Ø 支持 MAC 地址过滤
- Ø 支持 MAC 地址学习管理
- Ø 支持 MAC 地址老化管理
- Ø 支持基于端口的捕获
- Ø 支持强大 QoS 能力
- Ø 支持基于 WEB 的管理
- Ø 支持串口方式下的管理配置（仅限于恢复默认参数和升级）
- Ø 支持基于 WEB 方式的固件升级
- Ø 支持基于 X-Modem 的固件升级
- Ø 用户在交换上所作的配置参数可以备份到本地存储器上，然后根据需要随时恢复任何一个备份的配置参数

1.3. 支持的标准和协议

- Ø IEEE802.3 10BASE-T/802.3u 100BASE-TX
- Ø IEEE 802.3ab 1000Base-T 千兆以太网标准

- ANSI/IEEE 802.3x NWay 自动协商
- 10/100/1000M 速度全/半双工
- 全双工 IEEE 802.3x 流量控制
- IEEE 802.3Z 标准

1.4. 工作环境

温度

- 0° to 50° C（工作）
- -20° to 70° C（储存）

湿度

- 10% to 90 % 无凝结 (运行),
- 5% to 90% 无凝结 (储存)

电源

100-240V AC 50-60Hz

2. 硬件安装过程

2.1. 系统需求

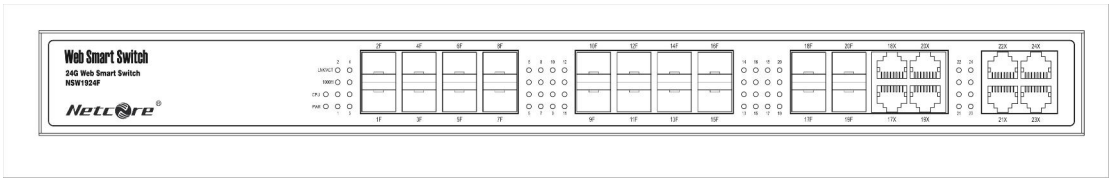
Ø 标准的个人计算机

Ø 操作系统微软 Windows，linux 操作系统

Ø 具备标准的 WEB 浏览器

2.2. 面板

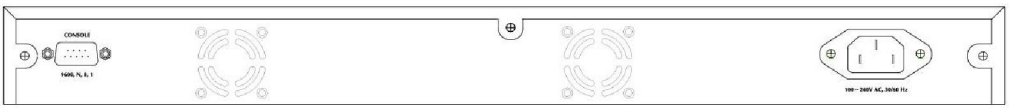
前面板



图片 2-1

LED	功能	
PWR	常亮	通电
	常灭	未通电
CPU	常亮	系统正常工作
LINK/ACT	闪烁	数据传输中
	常亮	对应端口连接正常
	常灭	对应端口连接断开
1000M	常亮	对应端口与所连接设备以 1000Mbps 速率工作
	常灭	工作在 10M/100M 模式

后面板



图片 2-2

CONSOLE：CONSOLE 端口。

电源：电源适配器插槽。

2.3. 硬件安装

安装前的准备

- Ø 放置交换机的表面必须至少能承重 4kg
- Ø 供电的电源插座距离交换机须在 1.8 米之内
- Ø 确保电源线两端已可靠地连接在交换机后面板上的电源接口和供电的电源插座
- Ø 保证交换机的四周可以良好的通风散热
- Ø 请勿将重物放置在交换机上

桌面安装过程

当欲将交换机安装在桌面上时，需先将包装箱内提供的 4个黏性胶垫粘贴在交换机底面的四角的相应位置，然后，再将交换机平放在桌面上，并确保交换机的周围能够良好地流动通风。

机架安装过程

首先，需要将包装箱内已提供的上机架的配件用与其配套的螺丝固定在交换机的前面板的两侧，然后，再用螺丝将交换机安装在 19英寸的机架内

电源

交换机的输入电压范围是 100-240 VAC（50-60Hz）的交流电，交换机的内置电源系统可以将实际输入的电压自动调整为其工作电压。电源接口位于交换机的后面板上，请将电源线一头插在交换机后面板上的电源接口上，另一头插在电源插座上。

3. 交换机的连接方法

3.1. 交换机的连接

交换机前面板提供 16个千兆 SFP光模块接口， 4个千兆光铜 combo和 4个千兆铜缆口，这些端口能自动侦测网络速度、自动适应双工状态。

本交换机能够连接工作站 PC、服务器、集线器、路由器、网桥、中继器或其他交换机。

3.2. 与网络最终节点的连接方法

连接网络终节点请用 3类或 3类以上的非屏蔽或屏蔽双绞线连接交换机 RJ-45接口和网络终节点 RJ-45接口。本交换机具有 AUTO-MDI/MDIX 自动线序交叉功能，直连线和交叉线都能连接本交换机。

- Ø 在 10Base-T 以太网必须使用 3 类或 3 类以上的屏蔽或非屏蔽双绞线。
- Ø 在 100Base-TX 快速以太网必须使用 5 类或 5 类以上的屏蔽或非屏蔽双绞线。
- Ø 在 1000Base-T 千兆以太网必须使用 5e 类屏蔽或非屏蔽双绞线。
- Ø 连接 1000M 光纤模块时，请使用 SFP 多模光纤

通过双绞线连接交换机与网络最终节点时双绞线的长度请不要超过 100米。

3.3. 与其它 HUB 或交换机的连接方法

将 NSW1924F与其他网络设备采用直联线或交叉线直接相连。

- Ø 10BASE-T 的 HUB 或交换机与交换机相连时，可以使用 3 类、4 类或者 5 类或以上的 UTP/STP 双绞线。
- Ø 100BASE-T 的 HUB 或交换机与交换机相连时，必须使用 5 类或以上的 UTP/STP 双绞线。
- Ø 1000BASE-T 的网卡或交换机与交换机相连时，必须使用超 5e 类或以上的 UTP/STP 双绞线。
- Ø 1000M 光纤模块与交换机相连时，请使用 SFP 多模光纤

4. 登入

你可以通过基于 web 浏览器的配置来管理 NSW1924F。要通过 web 浏览器配置 NSW1924F，至少要有一台合理配置的电脑，通过以太网连接到 NSW1924F。NSW1924F 的**默认 IP 地址是 192.168.2.11，子网掩码是 255.255.255.0**。所以在登录交换机之前，请确保电脑网卡的 IP 地址与交换机的 IP 处于同一网段：192.168.2.***（1<***<255，且***不等于 11）。参照下面步骤来设置

4.1. 配置电脑

4.1.1. Windows 98/Me

1、**开始－设置－控制面板**

2、找到并双击**网络**按钮，出现网络对话框

3、点击配置标签，并且确保你有网卡

4、选择 TCP/IP。如果 TCP/IP 出现的多于一个，请选择有箭头“ à ”的选项，它指向安装在你电脑上的网卡。**不要**选择旁边有“ 拨号适配器 ”的 TCP/IP

5、点击属性。出现 TCP/IP属性对话框

6、确保设置的是自动获取 IP地址

7、从 WINS的配置对话框，确保设置了禁用 WINS解析

8、从网关对话框，通过选择所有安装的网关，并且点击移除来移除所有入口

9、从 DNS配置对话框，通过选择搜寻 DNS命令块，并且点击移除来移除所有入口。通过从主要后缀搜寻命令块选择，并点击移除来移除所有入口。点击禁用 DNS

10、点击确定，返回网络配置对话框

11、点击确定，如果想立刻重启，点击是

4.1.2. Windows 2000

请按照下述步骤设置你的电脑

1、**开始－设置－控制面板**

图片 4-1

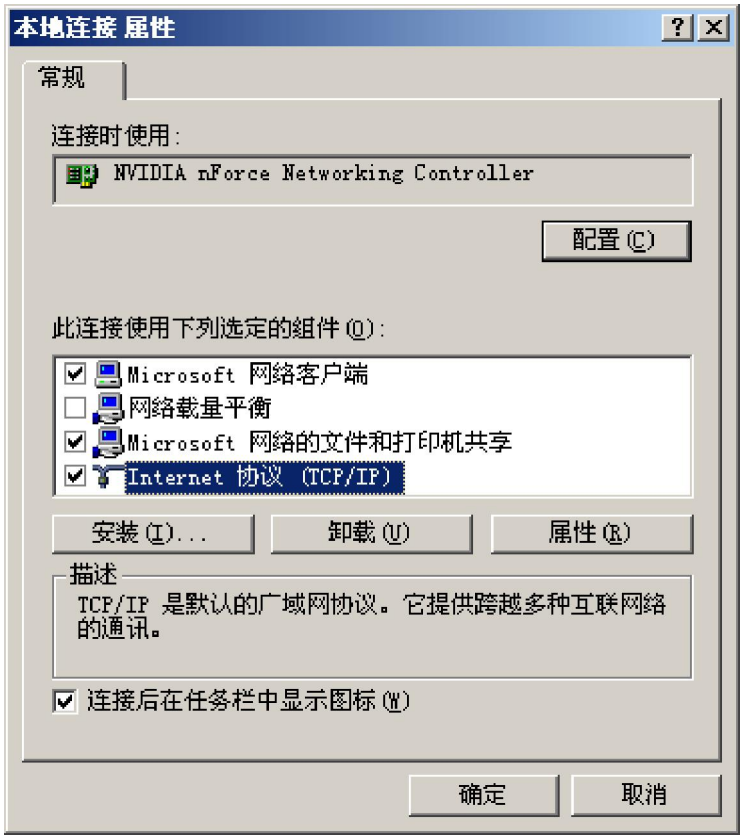
2、双击**网络和拨号连接**

图片 4-2

3、点击**本地连接**，右键选择**属性**

图片 4-3

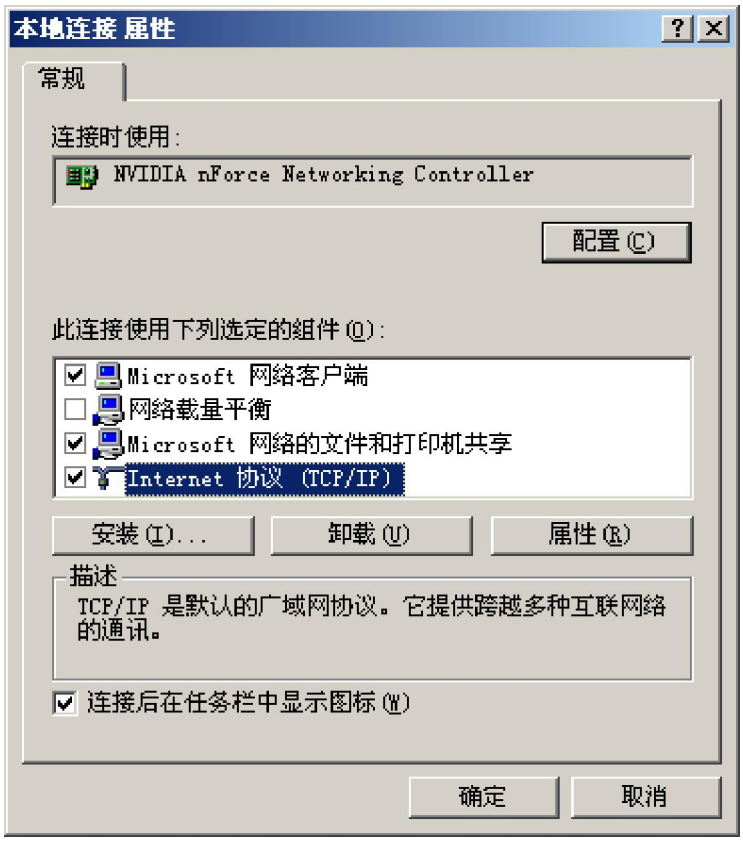
4、点击 **Internet 协议（TCP/IP）**，点击**属性**按钮



图片 4-4

5、选择**使用下面的 IP 地址**，输入 IP 地址为 **192.168.2.*****(1<*****<255，且*****不等于 11，因为**默认此交换机的 IP 地址为 192.168.2.11**)，**子网掩码 255.255.255.0**，默认网关和首选 DNS 服务器默认即可，然后点击确定，关闭 **Internet 协议（TCP/IP）属性**窗口

6、点击确定，关闭**本地连接属性**窗口



图片 4-5

4.1.3. Windows XP

请按照下述步骤来配置你的电脑

1、**开始－设置－控制面板**

图片 4-6

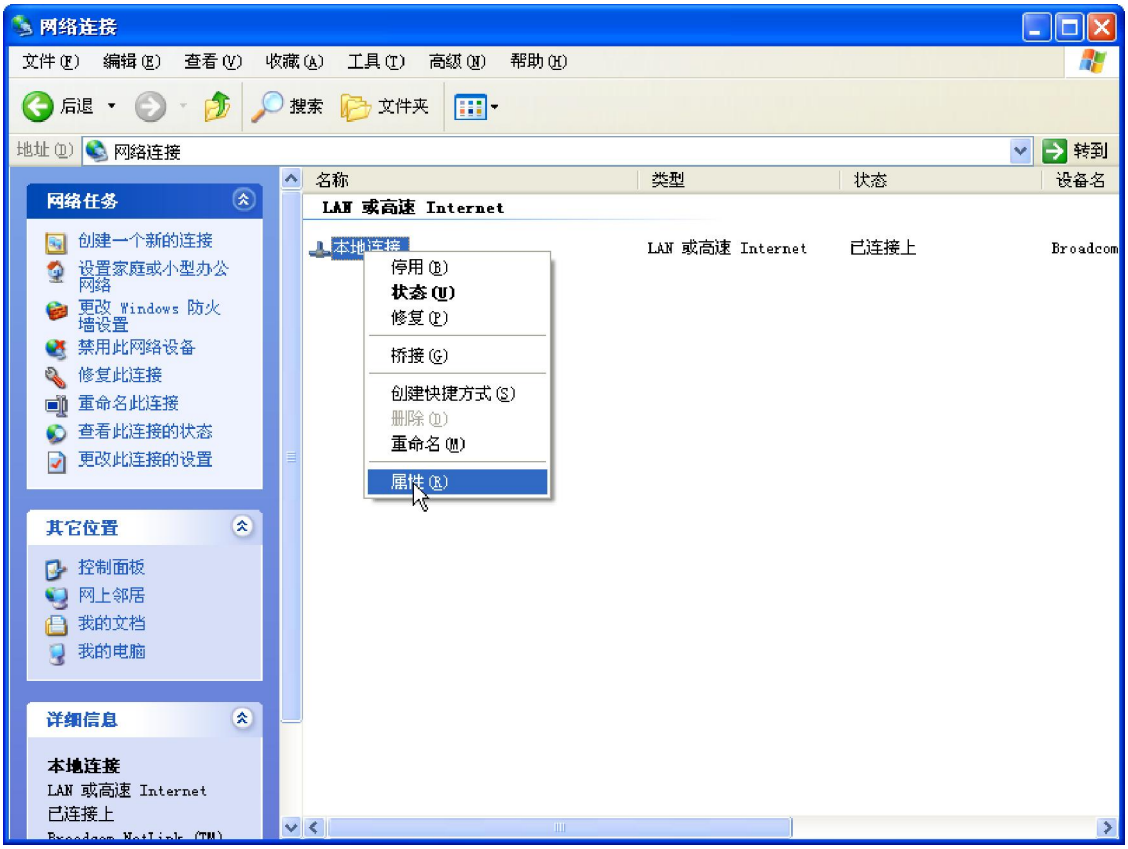
2、点击**网络和 Internet 连接**

图片 4-7

3、点击**网络连接**

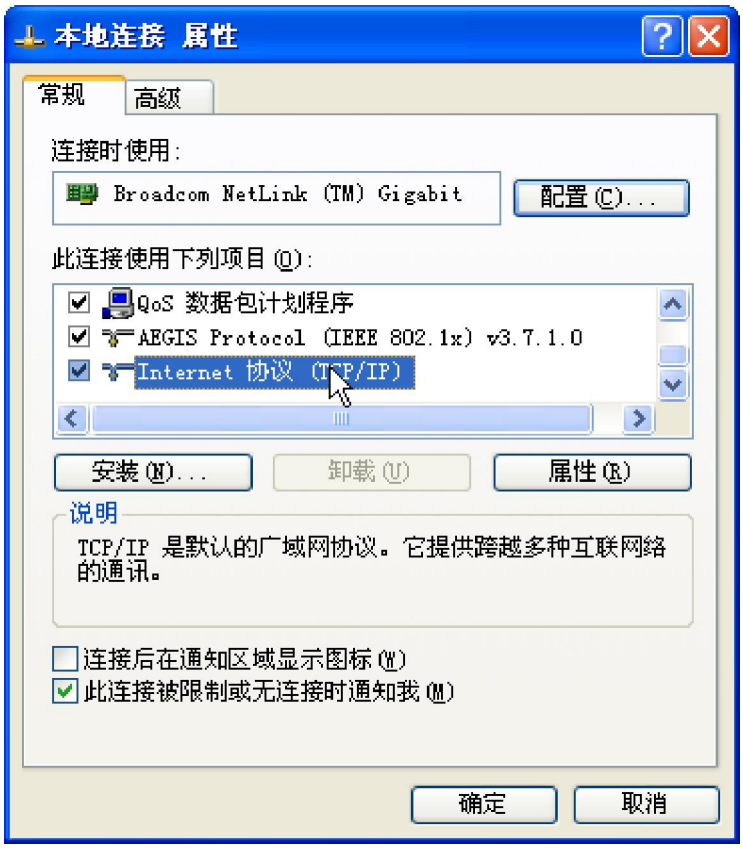
图片 4-8

4、点击**本地连接**，右键点击**属性**



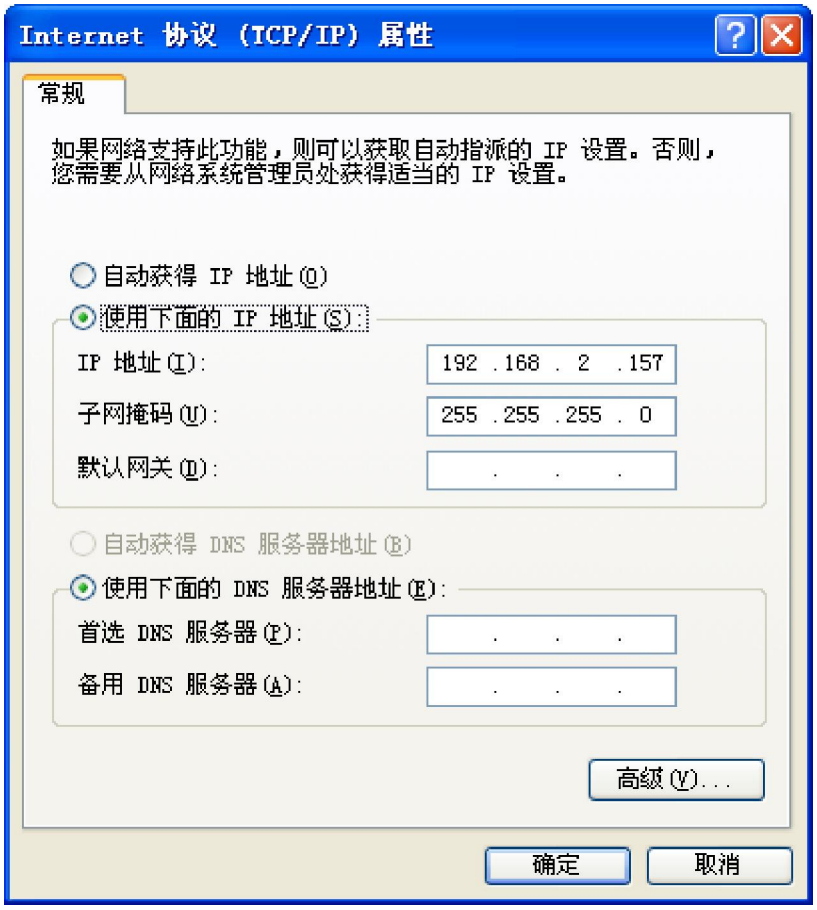
图片 4-9

5、点击 **Internet 协议（TCP/IP）**，点击**属性**按钮



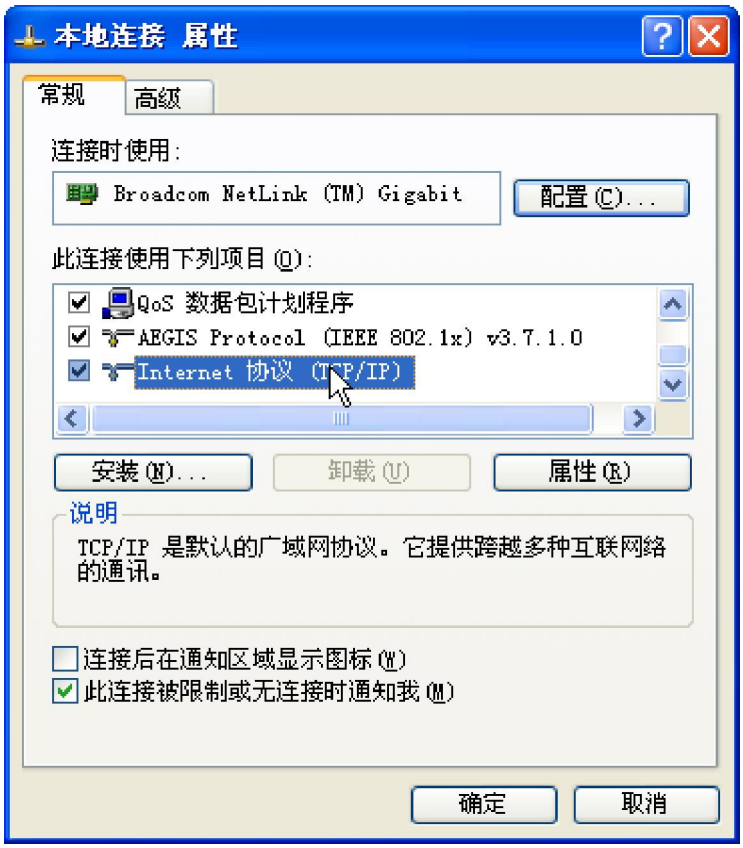
图片 4-10

6、选择**使用下面的 IP 地址**，输入 **IP 地址为 192.168.2. ***** (1<*******<255，且*******不等于11，因为**默认此交换机的 IP 地址为 192.168.2.11**)，**子网掩码 255.255.255.0**，默认网关和首选 DNS 服务器默认即可，然后点击确定，关闭 **Internet 协议（TCP/IP）属性**窗口



图片 4-11

7、点击**确定**，关闭**本地连接属性**窗口



图片 4-12

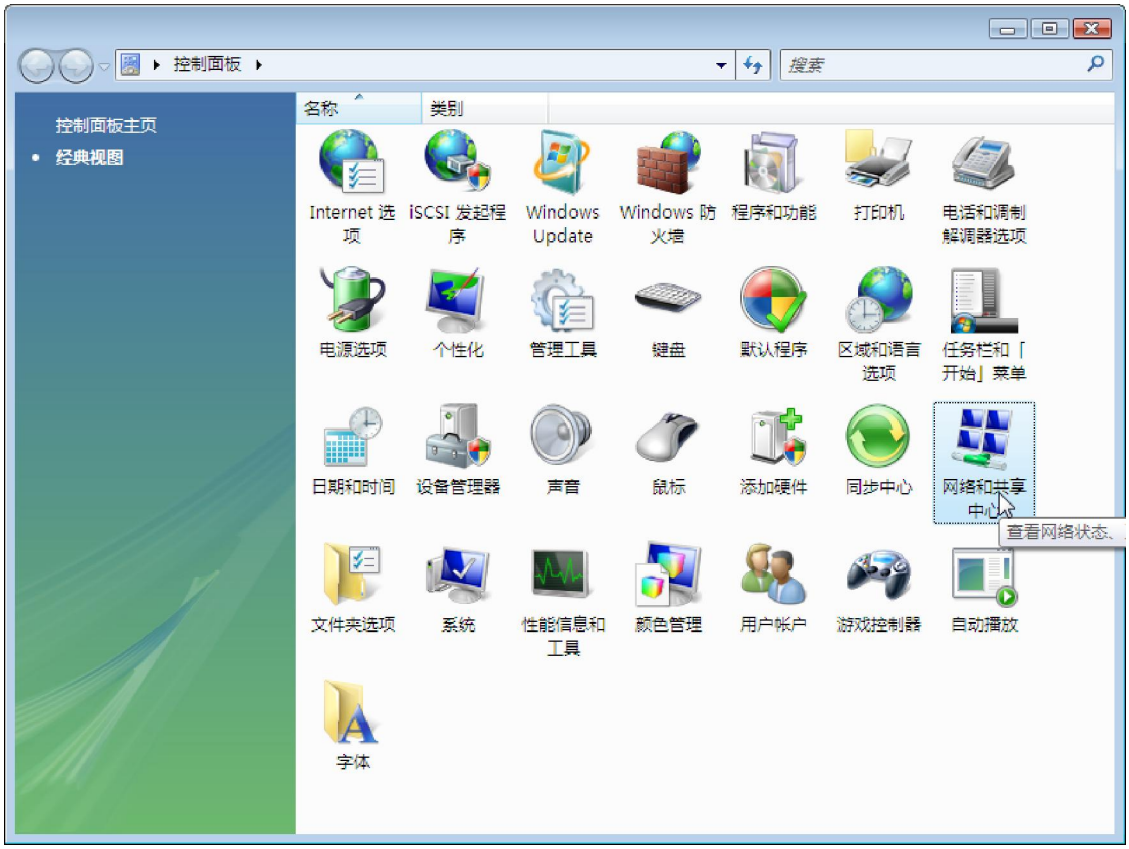
4.1.4. Windows Vista

请按照下述步骤配置你的电脑

1、**开始－控制面板**

图片 4-13

2、点击**网络和共享中心**

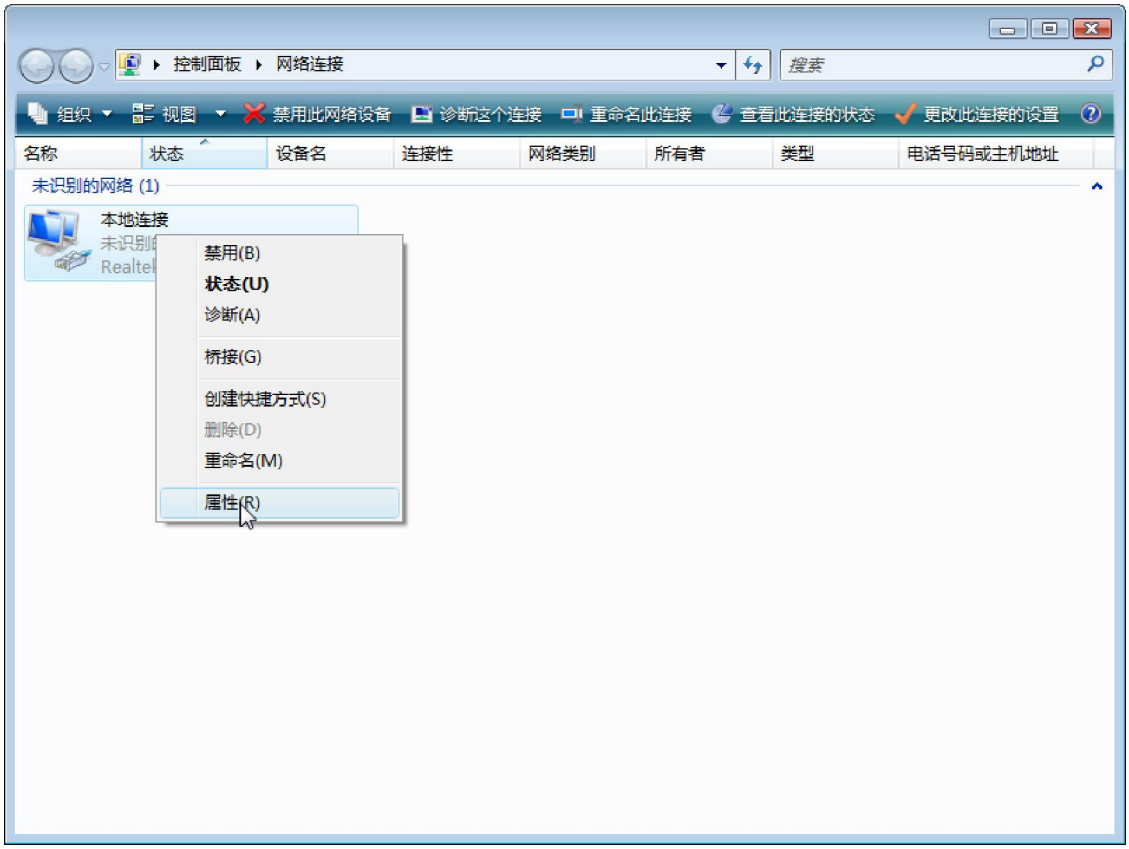


图片 4-14

3、点击**管理网络连接**

图片 4-15

4、右键点击**本地连接**，点击**属性**



图片 4-16

5、点击 **Internet 协议版本 4（TCP/IP）**，然后点击**属性**按钮

图片 4-17

6、选择**使用下面的 IP 地址**，输入 **IP 地址为 192.168.2. ***** (1<*******<255，且*******不等于11，因为**默认此交换机的 IP 地址为 192.168.2.11**)，**子网掩码 255.255.255.0**，默认网关和首选 DNS 服务器默认即可，然后点击**确定**关闭 Internet 协议（TCP/IP）属性窗口

7、点击确定关闭本地连接属性窗口

图片 4-18

4.2. 用 NSW1924F 检查电脑的 IP 和连接

设置完 TCP/IP 协议后，用 Ping 命令来验证电脑是否可以与 NSW1924F 通信。要执行 Ping 命令，打开 DOS 窗口，在 DOS 提示里 Ping NSW1924F 的 IP 地址

Ø 对 Windows 98/Me，开始－运行。输入 command 然后点击确定

Ø 对 Windows 2000/XP，开始－运行，输入 cmd 然后点击确定

在 DOS 提示里，输入下述命令

如果命令窗口返回类似于下面的内容

```
C:\Documents and Settings\admin>ping 192.168.2.11
Pinging 192.168.2.11 with 32 bytes of data:

Reply from 192.168.2.11: bytes=32 time=1ms TTL=64
Reply from 192.168.2.11: bytes=32 time=1ms TTL=64
Reply from 192.168.2.11: bytes=32 time=1ms TTL=64
Reply from 192.168.2.11: bytes=32 time=1ms TTL=64
```

```
Ping statistics for 192.168.2.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

那么 NSW1924F 和电脑之间的连接就成功的建立了

如果电脑没能连接上 NSW1924F，命令窗口将返回下述内容

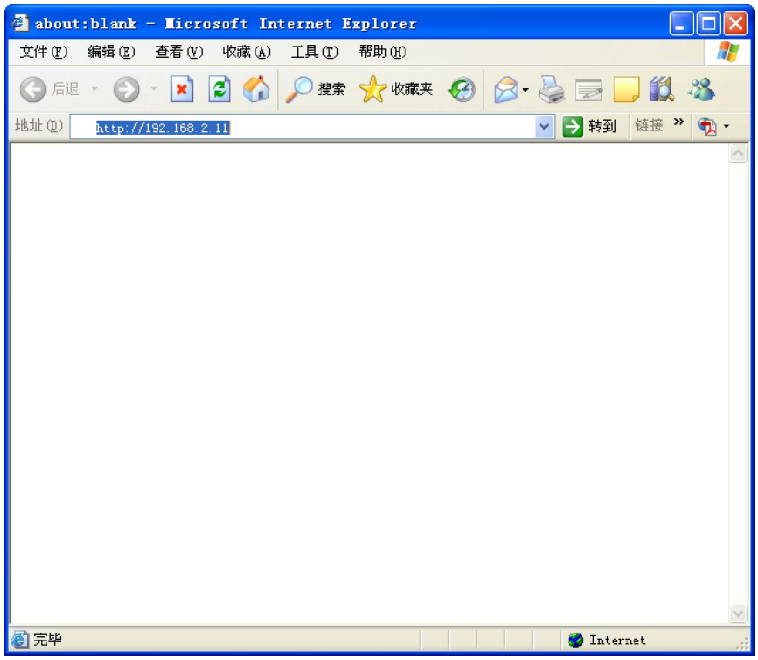
```
C:\Documents and Settings\admin>ping 192.168.2.11
Pinging 192.168.2.11 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

确认你电脑的网络设置是正确，并且检查 NSW1924F 与电脑之间的线路连接

为了使整个网络运行成功，有必要通过安装了 WEB 浏览器的电脑设置 NSW1924F。请按照以下步骤设置

4.3. 登入

1、打开 IE 浏览器，输入 http://192.168.2.11，点击 Enter



图片 4-19

2、在弹出窗口输入**用户名**：guest，**密码**：guest，按下**确定**键

图片 4-20

成功登录后，您就可以看到 NSW1924F 的 web 设置页面

图片 4-21

5. Web 设置

NSW1924F 支持 WEB 和 CONSOLE 控制台两种管理方式。

Web 设置页面包括以下几项内容：首页、系统管理、端口管理、冗余与备份、安全、QOS、组播管理、网络分析、网络设备保护、单 IP 管理。下面分别详细说明

5.1. 首页

当你成功登录后，您就可以看到此交换机的首页。首页显示了系统的基本信息。

图片 5-1

Ø 型号：

此设备的型号名称

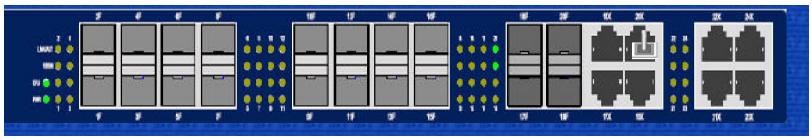
Ø MAC 地址：

这是此交换机的以太 MAC 地址

Ø 软件版本：

此交换机的固件版本信息

在右上角，显示了此交换机的前面板。在前面板上，连接的端口显示为绿色，未连接的端口显示为暗色。对可选模块（17－20）来说，插槽处如果有模块存在的话，则显示模块



图片 5-2

如图片 5-2 所示，我们可以看到现在正在用的是端口 20

点击此端口的图标，可以看到此端口的状态、接收包总字节数、接收包数、发送包总字节数、发送包数。

图片 5-3

5.2. 系统管理

系统管理包括：IP 地址、修改密码、MAC 地址、CONSOLE 信息、管理 VLAN、系统升级、参数保存、参数备份与恢复、恢复缺省参数、重新启动。下面详细说明

5.2.1. IP 地址

图片 5-4

在此页面您可以设置 IP 地址、子网掩码、网关和端口号。**默认 IP 地址是：192.168.2.11，默认子网掩码：255.255.255.0，默认网关 192.168.2.1**。修改完毕，点击确定后，完成 IP 地址的设置

5.2.2. 修改密码

图片 5-5

为 web 管理设置一个密码。

在首次登录此 web 界面时，为了安全起见，请在此修改密码。修改完密码后，在重新登录时，请使用新密码。默认密码是 **guest**

5.2.3. MAC 地址

图片 5-6

此处显示此交换机的 MAC 地址。您也可以修改这个值

5.2.4. CONSOLE 信息

图片 5-7

显示 console 设置信息

5.2.5. 管理 VLAN

图片 5-8

VID，即 VLAN ID，您可以输入 1-4094 之间的数字。通过管理 VLAN 限制只能设置属于此 VLAN 的端口才能登录交换机进行配置。不启用则所有 VLAN 下面的端口都能同时登陆交换机进行配置。

例如：限制属于 VID 为 1 主机才能登陆交换机进行配制。

注意：管理 VLAN 只对 QVLAN 生效（我们通常将 802.1Q VLAN 简称为 QVLAN）

5.2.6. 系统升级

图片 5-9

通过此处的功能可以在本地对此交换机进行升级。点击“ 浏览 ”，选中保存在本地的升级文件后，选中“ 开始升级 ”，开始自动升级。

注意：在升级过程中，请不要拔掉电源，否则将会导致升级失败

5.2.7. 参数保存

图片 5-10

点击“ 参数保存 ”，则会自动保存当前交换机上所配置的系统参数，重启交换机后，这些配置参数仍然生效。如果不做参数保存的话，当前配置的参数仅在此次配置上生效，下次重新启动后，配置的参数将会丢弃

注意 如果想让此次设置的参数在以后重新登录系统的时候仍然有效，请及时进行参数保存。否则，下次登录系统后，参数将全部丢失

5.2.8. 参数备份与恢复

图片 5-11

Ø 备份当前交换机的所有参数配置，以便以后的恢复操作：

点击此按钮，则会保存一个文件到您的电脑。

Ø 参数恢复

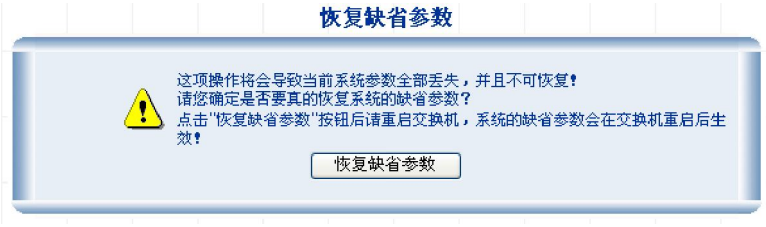
点击下方的“浏览”，选择正确的备份文件后，点击确定，则交换机会自动恢复参数

图片 5-12

参数恢复成功后，有提示

图片 5-13

5.2.9. 恢复缺省参数

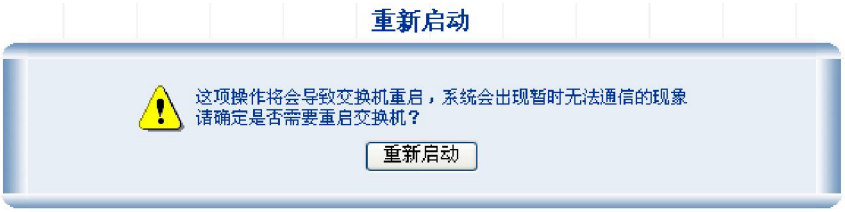


图片 5-14

点击“ 恢复缺省参数 ”，交换机会自动恢复到出厂设置。

注意：此项操作将会导致交换机丢失所有当前保存的参数配置，除非遇到严重的问题，且在任何其他办法都无效的情况下，请慎重选择

5.2.10. 重新启动



图片 5-15

点击“ 重新启动 ”，则交换机自动重启

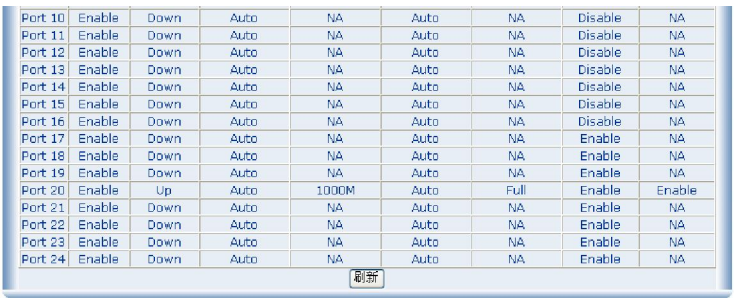
5.3. 端口管理

端口管理包括：端口配置、端口统计、端口带宽限制、级联口配置、线缆测试、缓存调度策略。下面详细说明

5.3.1. 端口配置

显示各个端口的状态信息。

图片 5-16



图片 5-17

Ø 端口配置

建议使用默认配置，但您也可以在此更改某一些端口的状态信息.

Ø 查看端口状态

² 管理状态

有 enable 和 disable 两种状态。可以在端口配置里面更改

² 连接状态

有 down 和 up 两种状态。其中 down 是端口没有连接，up 是端口处于连接状态

² 速度/双工

设置端口的传输速度和全双工/半双工。默认是自动协商 auto，它能够自动侦测到网络速度、双工状态，并根据网络情况调整自己的传输速度以及双工状态以达到最高的传输速度。

² 流量控制

Enable 或 disable 端口的流量控制。默认是 disable。流量控制功能要求所连接的设备必须支持 IEEE 802.3x 且可以以全双工的方式传输，当交换机上的缓冲区被存贮满，交换机将发送 Pause 帧，通知发送方设备暂停发送数据。用户可通过“ 流量控制 ”框，来设定是否打开流量控制功能。

5.3.2. 端口统计

显示端口统计信息

图片 5-18

图片 5-19

Ø 点击刷新，可以显示此刻的端口统计信息

Ø 点击“复位统计信息”，则发送、接收包数等信息被清空

5.3.3. 端口带宽限制

如果有网刻，请不要设置端口带宽限制

图片 5-20

在此可以看到端口带宽的状态信息。包括端口号、入口限制种类、入口限制带宽、出口限制带宽。

图片 5-21

可以在此更改某一个端口的限制种类、入口带宽限制和出口带宽限制，点击增加，即可改变此端口的信息。如图片 5-21 所示

图片 5-22

图片 5-22 为端口 2 被更改后的显示信息

5.3.4. 级联口配置

图片 5-23

显示级联口配置信息。从左边桥端口列表选择某一个端口，点击添加，即可添加到右边的级联口列表，从右边的级联口列表选择某一个端口，即可删除。

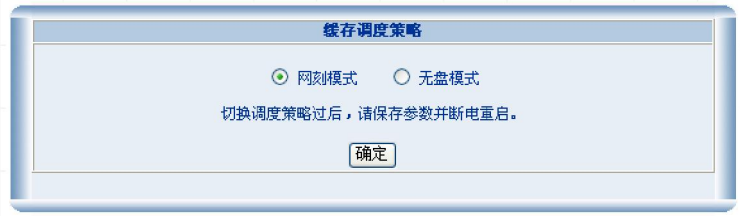
级联口是为了便于两台交换机之间进行级联的端口。如果您想用端口 20 与其他交换机进行级联，请在左边选择端口 20，添加到级联口列表中。如果您将端口 20 设置为级联口，则会把端口 20 上接的设备看成是同级设备。

5.3.5. 线缆测试

图片 5-24

可以对每一个端口进行线缆测试。请注意一次只能测试一个端口

5.3.6. 缓存调度策略



图片 5-25

您可以选择网刻模式和无盘模式。请根据具体需要选择不同的模式

网刻，即网络克隆，是用 TFTP 协议，通过 ghost 服务器刻硬盘的，一般的用来刻系统，优点在于操作简单，不用开机箱。适合没用光驱的网吧机器以及公司机器

无盘，即无硬盘。在网内有一个系统服务器，这台系统服务器上除了有它本身运行所需的操作系统外还需要有一个工作站运行所需的操作系统。无盘工作站的机箱中没有硬盘，其它硬件都有，而且无盘工作站的网卡必须带有可引导芯片。在无盘工作站启动时网卡上的可引导芯片从系统服务器中取回所需数据供用户使用

5.4. 冗余与备份

冗余与备份只有一个选项，即链路聚合

5.4.1. 链路聚合

链路聚合是将两个或更多数据信道结合成一个单个的信道,该信道以一个单个的更高带宽的逻辑链路出现。链路聚合一般用来连接一个或多个带宽需求大的设备，例如连接骨干网络的服务器或服务器群。

图片 5-26

从上方的聚合组选择一个端口，然后从左边的端口列表选择 n 个（n>=0）端口，点击增加，加入到聚合组的端口。如果不想加入，则选择加入聚合组端口的端口号，选择删除，即可删除。在端口加入了聚合组以后，即相当于此端口更改为聚合组。例如如果从端口列表选择了

端口 1、2、3 加入聚合组 25，则在查看端口 1、2、3 时，均显示端口 25，而端口 1、2、3 不可见。

聚合组总共有 12 个，从 port25 到 port36，而一个聚合组可以加入的最多端口数为 8 个

例如：如果我们想在 NSW1924F 上同时设置 2 个端口聚合，每个端口工作在 1000M 全双工方式下。这样配置的效果是：得到了一条双向 4000M 带宽的逻辑链路

第一步：在“链路聚合”页面中的聚合组选择 port25（port25-port36 表示聚合组 1-12）

第二步：在交换机 1 的链路聚合配置中，选择端口列表中的 port3、port5，单击增加按钮，将 port3、port5 端口加入到聚合组 1（port25）中

第三步：在交换机 2 上重复第二步，将 port3、port5 加入聚合组 1（port25）

5.5. 安全

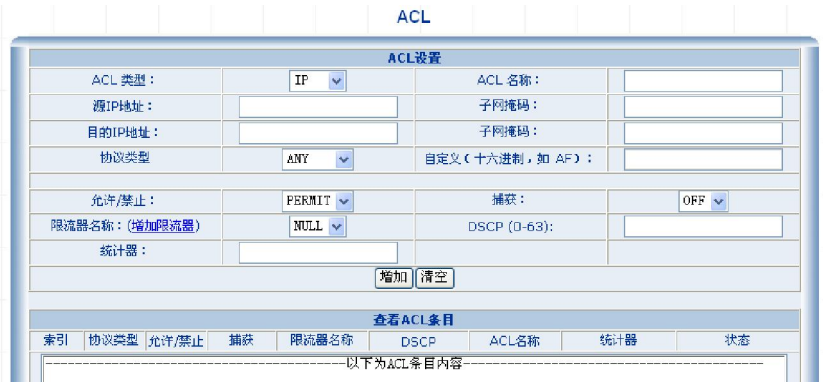
安全包括：ACL、安全防御、ARP 攻击防御、网络防水墙、VLAN、MAC 地址绑定、MAC 地址过滤、MAC 地址学习、MAC 地址老化。下面详细说明

5.5.1. ACL

网络设备为了过滤数据包需要配置一系列的匹配规则以识别需要过滤的对象，在识别出特定的对象后，才能根据预先设定的策略允许或禁止相应的数据包通过。访问控制列表 Access Control List(ACL)就是用来实现这些功能的

ACL 通过一系列的匹配条件对数据包进行分类，这些条件可以是数据包的源地址、目的地址、端口号等。ACL 应用在交换机全局或端口，交换机根据 ACL 指定的条件来检测数据包从而决定是转发还是丢弃该数据包由 ACL 定义的数据包，匹配规则还可以被其他需要对流量进行区分的场合引用如 QOS 中流分类规则的定义

NSW1924F 的 ACL 条目是由下向上匹配的，基于 MAC 地址匹配级别高于其他协议类别



图片 5-27

Ø ACL 设置

² ACL 类型：

包括：MAC、IP、TCP、UDP、ICMP。请根据所需选择 ACL 的类型，默认为 IP。在 IP 类型下，要填写源 IP 地址/目的 IP 地址、子网掩码和协议类型；在 MAC 类型下，要填写源 MAC 地址/目的 MAC 地址；在 TCP/UDP 类型下，要填写源 IP 地址/目的 IP 地址、子网掩码、源端口/目的端口；在 ICMP 类型下，要填写源 IP 地址/目的 IP 地址、子网掩码

² ACL 名称：

为此 ACL 取的名字，便于识别。

² 允许/禁止：

可以选择 PERMIT 或 DENY。如果您要允许，请选择 PERMIT

² 捕获：

可以进行限定流的捕获。在 ACL 列表中查看是否开启了捕获，如果开启了，则满足该条件的报文会复制一份发送到 CAPTURE 端口。

² 限流器名称：

可对本设定的流进行速度的限制。默认为空 NULL。如果您想增加限流器，请点击“ 增加限流器 ”，如图片 5-28 所示。则在弹出框图片 5-29 输入对限流器的配置，这些配置就会在图片 5-29 下方的查看 QoS 限流器列表中出现

图片 5-28

图片 5-29

² DSCP：

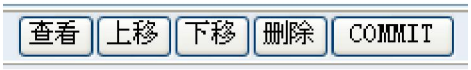
DSCP 是差异化服务编码点，请在此框中输入 0-63 之间的数字

² 统计器：

输入统计器的名称。可以对该流进行数据统计，在“ 网络分析－QOS 统计器 ”中查看

ACL 设置下方有 2 个按钮“ 增加 ”与“ 清空 ”。当填写完成一个 ACL 条目时，点击“ 增加 ”，则此项信息被添加到下方的 ACL 条目中。您可以点击“ 清空 ”按钮来清空所填写的信息。

Ø 查看 ACL 条目



图片 5-30

在查看 ACL 条目列表下方，可以看到图片 5-30。点击“ 查看 ”可以查看 ACL 列表中选定的某一个 ACL 条目的详细信息。点击“ 上移 ”/“ 下移 ”可以使选中的 ACL 条目向上/下移动一位。点击“ 删除 ”可以删除选中的 ACL 条目。点击“ COMMIT ”可以使选中项的状态变为 COMMIT，在新增了一个 ACL 条目的时候，默认状态为 UNCOMMIT，需要手动在此更改状态

5.5.2. 安全防御

图片 5-31

Ø 安全防御模板设定

² 安全防御模板：

包括蠕虫、RPC 漏洞、震荡波、Tftp、冲击波和 Phatbot

Ø 用户定义安全防御

² 名称：

为此安全防御取一个名字，便于识别

² 协议：

可以勾选 TCP 和 UDP。当勾选了其中之一时，需要填写端口号

Ø 查看安全防御条目

当您在用户定义安全防御填写了名称，选择了协议后，此处就显示出条目信息。

5.5.3. ARP 攻击防御

该设置用于定时发送路由器 ARP Response，以保护没有直接连接本交换机的主机到路由器的连通性，最多支持 6 台路由器（填 0 表示取消设置）

注意：在 PortBased VLAN 和 IEEE 802.1Q VLAN 之间切换后，请重设此功能

图片 5-32

Ø ARP 攻击防御保护时间：

填写 10－3000ms 之间的数字

5.5.4. 网络防水墙

图片 5-33

图片 5-34

Ø 报告机制设置

- 启用报告机制：

当需要启用报告机制时，可以勾选此项启用报告机制

Ø 网管 IP 设置

- 网管 IP 地址：

在此输入网管的 IP 地址

Ø 报文广播类型：

包括：ARP 防御精灵和防水墙。

Ø 加密 ARP 信息广播

- 广播时间：

在此填写广播时间：10－60s 之间的一个数字

5.5.5. VLAN

VLAN是一种通过将局域网内的设备逻辑地(而不是物理地)划分成一个个网段，从而实现虚拟工作组的技术。为了建立起安全的、独立的广播域或者组播域，可以将交换机上的端口组合成多个虚拟局域网（VLAN）。设置VLAN的主要目的是为了限制广播包的传播范围和降低广播包的影响。所有以太网数据包，如单播（unicast）、组播（multicast）、广播（broadcast），以及未知（unknown）的数据包，都将只在VLAN内传送。这样在一定程度上，可以提高网络的安全性。

VLAN的另一个优点是可以改变网络的拓扑结构，但并不需要网络中的工作站发生物理上的移动或者网络线路连接上的变动。可以仅仅改动工作站的VLAN设置，就可将工作站从一个VLAN（如销售部VLAN）“移到”了另一个VLAN（市场部VLAN）这可使网络节点的移动、变换、增加变得非常灵活和容易。

此交换机支持 802.1Q VLAN 和 Port-Based VLAN。VLAN 配置能够按照您的需要将 LAN 划分成小块。正确地配置它，就能够提高安全性，改善性能并且能极大的减少 VLAN 管理

Ø VLAN 类型：

VLAN 有两种类型：802.1Q VLAN 和 Port-Based VLAN，您可以选中其中之一，然后点击确定使其生效

5.5.5.1. 802.1Q VLAN

802.1Q协议，即 Virtual Bridged Local Area Networks协议，主要规定了 VLAN的国际标准，内容是一种在逻辑上划分网络桥接的局域网结构，并提供定义用户组在跨越不同交换设备 VLAN之间的连接服务，这使得不同厂商之间的 VLAN互通成为可能。VLAN的最大数目也不受交换机端口数目的限制，最大可达到 4094个。

在 802.1QVLAN中，网卡（NIC）不必去识别数据包头部分的 802.1Q标记（tag），网卡只需发送和接收普通的以太网数据包。TAG的信息由交换机的端口根据相应的 PVID加入到数据包中。交换机根据包头中的 TAG信息决定如何转发这个数据包。

在理解 IEEE 802.1QVLAN时，有两个非常重要的名词需要掌握，就是端口 VLAN的 ID（Port VLANID numbers 简写为 PVID）和 VLAN的 ID（VLANID numbers 简写为 VID）。这两个变量都是定义在端口上的，但是两者间有很大的区别。用户可以仅为每个交换机端口定义一个 PVID，PVID 定义了交换机将向哪一个 VLAN转发数据包，以及什么时候数据包会需要转发到另一台交换机的端口上，或者网络中的某个地方。另外，用户也可以定义某个端口同时属于多个 VLAN（即 VIDs），使得它可以接收网络中多个 VLAN的数据包。PVID 和 VID 这两个变量用于控制端

口发送和接收 VLAN 数据流的能力，而两者之间的区别在于后者还允许信息可以在多个 VLAN 间共享。

802.1Q VLAN 是由 VID 决定的，全然不同于 Port-Based VLAN。如果有任何更多的入口过滤规则列表或出口过滤规则列表，数据包将被甄别更多的筛选条件来确定是否可以转发。您建立的每一个 802.1q VLAN 都必须分配 VLAN 名字和 VLAN ID。合法的 VLAN ID 范围是 1— 4094

图片 5-35

802.1QVLAN 是默认设置。选择后点击确定，则您可以看见所有端口的 VLAN 信息显示

802.1Q VLAN

端口	链路类型	PVID	出口规则
Port1	Access	1	Untagged=1
Port2	Access	1	Untagged=1
Port3	Access	1	Untagged=1
Port4	Access	1	Untagged=1
Port5	Access	1	Untagged=1
Port6	Access	1	Untagged=1
Port7	Access	1	Untagged=1
Port8	Access	1	Untagged=1
Port9	Access	1	Untagged=1
Port10	Access	1	Untagged=1
Port11	Access	1	Untagged=1

图片 5-36

交换机的 802.1Q 配置是基于每一个端口来配置所属的 VLAN 信息的

点击某一个端口可以修改此端口的 VLAN 配置。例如点击端口 1，出现 VLAN 端口配置信息

图片 5-37

链路类型包括 Access、Trunk和 Always Untag，下面是对一些常用术语的说明

Ø Tagging

将 802.1QVLAN的信息加入数据帧头。具有加标记能力的（tagging enabled）端口会将 PVID、优先级和其它 VLAN信息加入到所有进出该端口的数据帧中。如果在此前数据包已经被做过标记，端口将不对该数据包进行改动，让其保持其已有的 VLAN信息。标记（Tagging）使得数据包能够从一台支持 802.1Q的交换机能够传送到另一台同类的交换机上。

Ø Untagging

将 802.1QVLAN的信息从数据帧头去掉。具有去标记能力的（untagging enabled）端口会将 VID、优先级和其它 VLAN信息从所有进出该端口的数据包包头中去掉。如果在此前数据包内没有被标记过，端口将不对该数据包进行改动。去标记（Untagging）使得数据包能够从一台支持 802.1Q的交换机传送到其它不支持 802.1Q的交换机上。

Ø Access 链路

即 Untagging，是将 802.1QVLAN 的信息从数据帧头去掉。具有去标记能力的（untagging enabled）端口会将 VID、优先级和其它 VLAN信息从所有出该端口的数据包包头中去掉。如果在此前数据包内没有被标记过，端口将不对该数据包进行改动。去标记（Untagging）使得数据包能够从一台支持 802.1Q的交换机传送到其它不支持 802.1Q的交换机上。

Ø Trunk链路

是将某端口设定为对某一个 VLAN的数据帧 Untagging，而对其他您所选定的 VLAN的数据帧 Tagging，Tagging 是将 802.1QVLAN 的信息加入数据帧头。具有加标记能力的（tagging enabled）端口会将 PVID、优先级和其它 VLAN信息加入到所有进出该端口的数据帧中。如果在此前数据包已经被做过标记，端口将不对该数据包进行改动，让其保持其已有的 VLAN

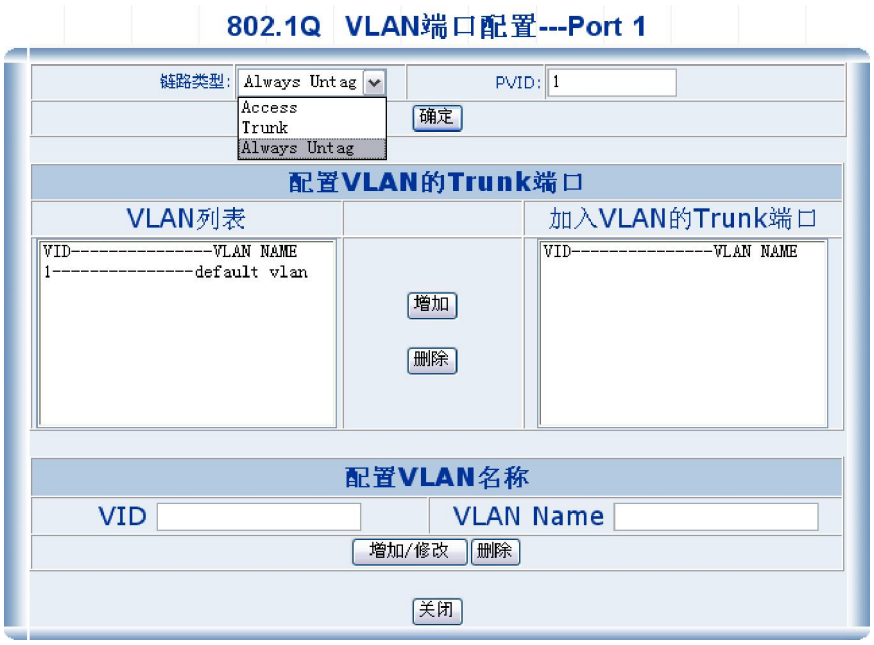
信息。标记（Tagging）使得数据包能够从一台支持 802.1Q的交换机能够传送到另一台同类的交换机上。

Ø PVID

是端口所属的 VID号。

Ø 下面对功能 Always Untag进行详细说明：

NSW1924F有一个Always Untag的功能。如果是遇到trunk链路的，也同样是去掉tag头，按always untag来配置。



图片 5-38

下面具体应用来说明此功能：

目前有一些应用，将局域的划分为几个 VLAN，让各自 VLAN 中的机器不能互相访问，但是网络中有一台公用的服务器，所有设备又都能访问服务器。

主机 A、B、C 分别位于交换机 2、3、4 端口，服务器接在 5 号端口。要实现 A、B、C 不能互相访问，但又能同时访问服务器，我们应该怎么设置 VLAN 呢？

配置思路：

需要配置四个 VLAN

VLAN	成员端口
VLAN2	2、5
VLAN3	3、5
VLAN4	4、5
VLAN5	2、3、4、5

端口	PVID

5	5
2	2
3	3
4	4

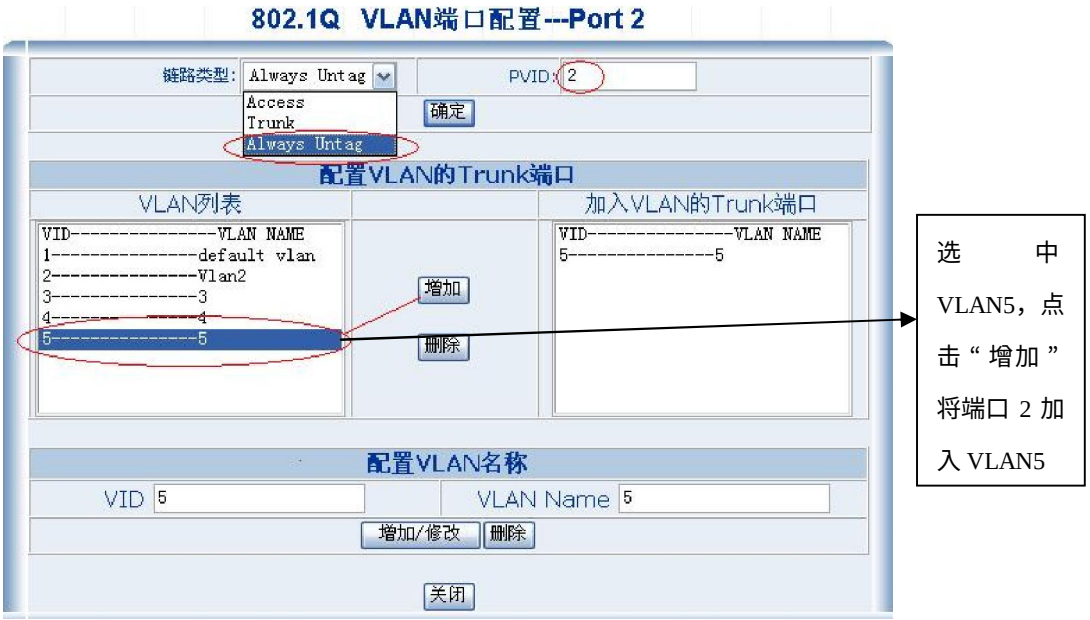
1、建立 VLAN2、VLAN3、VLAN4、VLAN5

2、端口 2 的配置方法：

将 port2 的 PVID 设置为 2

将链路类型设置为：Always untag

将端口 2 加入到 VLAN5 中



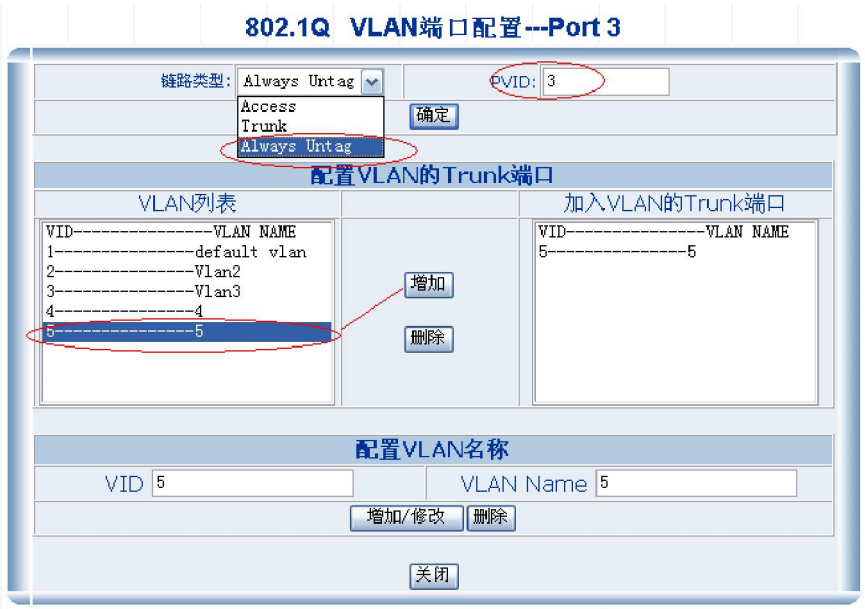
图片 5-39

3、端口 3 的配置方法：

将 Port 3 的 PVID 值设置为 3

链路类型为：Always untag

将端口 3 加入到 VLAN5 中



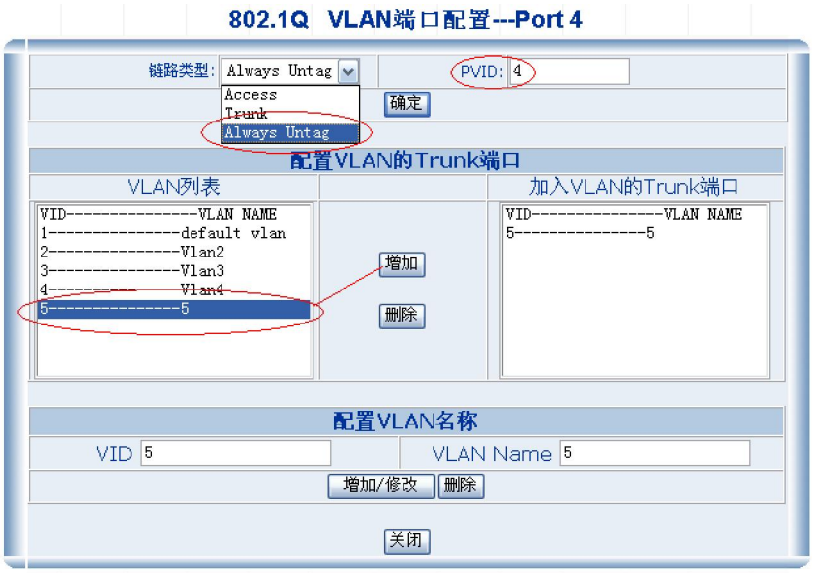
图片 5-40

4、端口 4 的配置方法：

将 Port 4 的 PVID 值设置为 4

链路类型为：Always untag

将端口 4 加入到 VLAN5 中



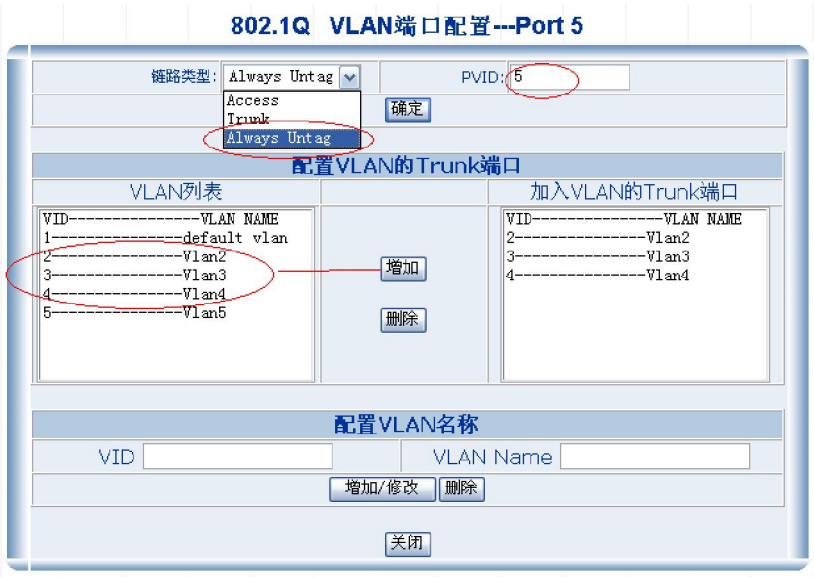
图片 5-41

5、端口 5 的配置方法：

将 Port 5 的 PVID 值设置为 5

链路类型为：Always untag

将端口 5 加入到 VLAN2、VLAN3、VLAN4 中



图片 5-42

下面是对某一个端口的端口配置页面的具体说明

配置 VLAN名称

图片 5-43

点击“增加/修改”后，新增的 VLAN会显示在 VLAN列表中

图片 5-44

交换机默认将 PVID与 VID与 VLAN 对应。 PVID=2 相当于将一个端口设置为 VLAN2 的成员要将此端口加入一个 VLAN，可以选择链路类型，例如为 PVID为 2的端口选择 Trunk后，则此时已将端口 2配置为 VLAN2的成员

图片 5-45

返回前页，查看 VLAN成员，即可查看到该交换机的 802.1QVLAN成员信息

举例说明 802.1Q VLAN的应用

例： PC1与 PC3属于同一 VLAN ； PC2与交换 2上某一台机器属于同一 VLAN

分析：根据需求需要创建两个 VLAN ：VLAN2和 VLAN3，假设 PC1在 Port1上；PC2 在 port3上， HUB接在 Port2上。需要将端口 1、 2加入 VLAN2；将端口 2、 3加入 VLAN3（端口 2既

属于 VLAN2又属于 VLAN3)。并且让从端口 2出去的 VLAN2的数据 Untagging (因为 PC只能接受不带 tag头的包) 对 VLAN3的数据 tagging, 也就是将 Port2的链路设置为 Trunk链路，即要传输带 tag的包又要传输不带 tag头的包。

Ø 首先创建 VLAN2和 VLAN3

图片 5-46

创建 VLAN3类似。

Ø 配置端口 1

将端口 1配置为 VLAN2, 将端口 1的 PVID设置为 2，系统会自动加端口 1加入 VLAN2，因为端口 1直接接 PC, 链路应该设置为 Access

图片 5-47

Ø 配置端口 3

将端口 3配置为 VLAN3, 就是将端口 3的 PVID设置为 3，系统会自动加端口 3加入 VLAN3，因为端口 3直接接 PC, 链路应该设置为 Access

图片 5-48

Ø 配置端口 2

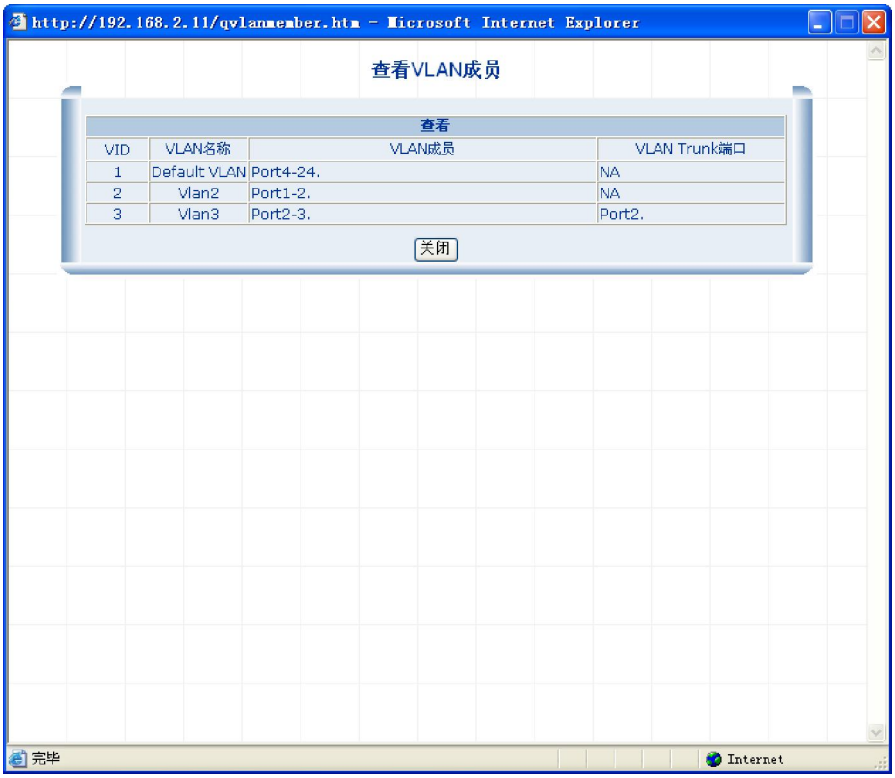
先将链路类型设置为 Trunk，再配 PVID，由于端口 2同属于 VLAN2和 VLAN3，那么 PVID应该怎么配呢？如果将 PVID配置成 2，那么系统会自动将从该端口出去的 VLAN2的数据都不带 tag头，而需求要求 VLAN的数据是不能带 tag头的，所以将 PVID配置成 2，需求要求 VLAN3的数据要带 tag，那么需要在“配置 VLAN的 Trunk端口”中选中 VLAN3，这样 VLAN3的数据从端口 2出去时是带 tag的数据。

图片 5-49

Ø 配置完成后可以去查看所有 VLAN的配置信息

图片 5-50

Ø 再查看 VLAN的成员列表



图片 5-51

5.5.5.2. Port-Based VLAN

Port-Based VLAN 是由任意端口决定的。从 Port-Based VLAN 输入和输出的任意包都将被接受。过滤标准均不适用于 Port-Based VLAN。唯一的标准是您连接的物理端口。例如：一个叫 PVLAN1 的 Port-Based VLAN 包含端口 1、2、3、4，如果您在端口 1，可以与端口 2、3、4 通话。如果您在端口 5，就不能与任意一个通话。您建立的每一个 Port-Based VLAN 都必须分配一个群组名称。

此页面显示已存在的 Port-Based VLAN 组的信息。点击“ 增加/修改 ”按钮，您可以很容易

的增加、修改一个 Port-Based VLAN 组。增加一个 Port-Based VLAN 组后，可以很容易地得到所有的 VLAN 成员信息

图片 5-52

Ø VLAN 名称：

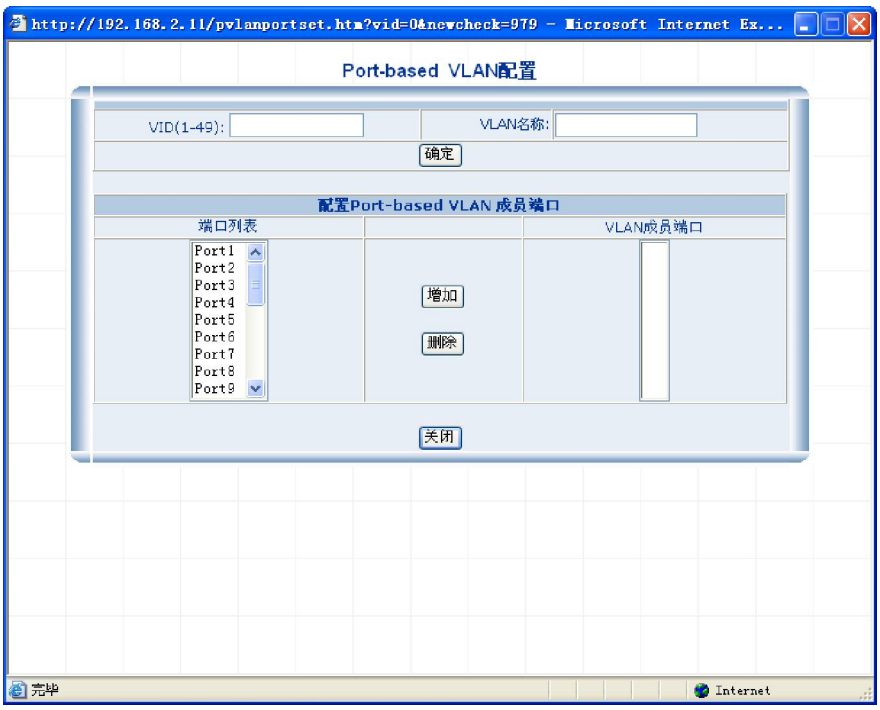
与 VLAN 组相关的 VLAN 名称

Ø VID：

VLAN ID

Ø 增加/修改：

可以增加一个新的 Port-Based VLAN 组或者修改一个 Port-Based VLAN 组配置



图片 5-53

Ø 端口列表：

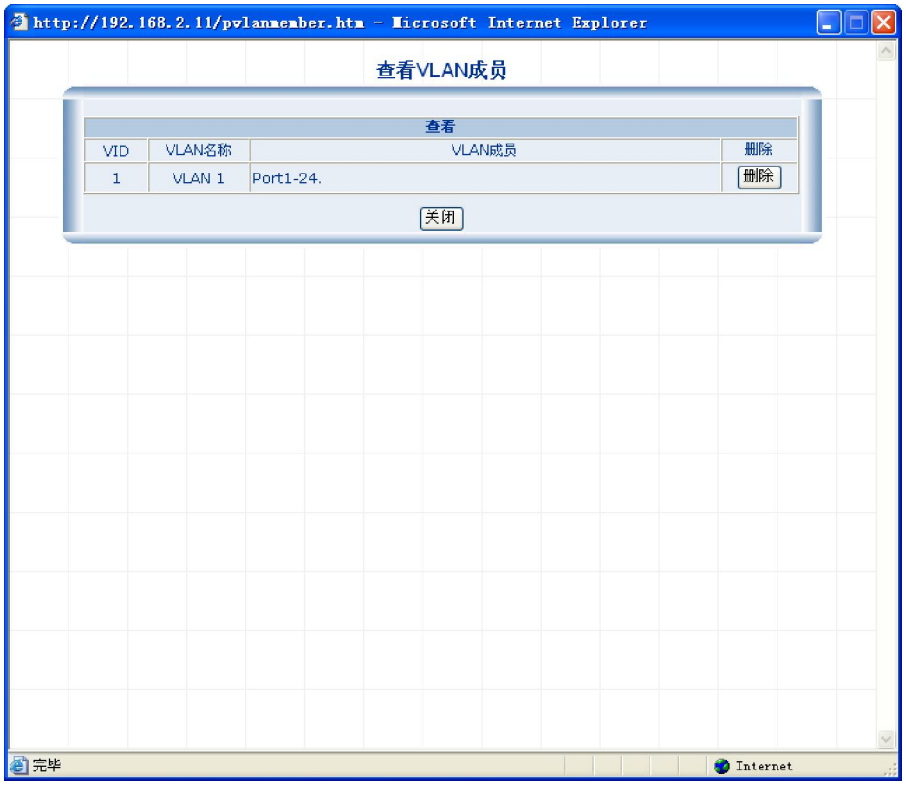
显示此交换机的所有端口

Ø VLAN 成员端口：

显示 VLAN 组的所有成员端口

Ø 查看 VLAN 成员：

查看 VLAN 组的 VLAN 成员



图片 5-54

5.5.6. MAC 地址绑定

MAC 地址绑定是 NSW1924F 支持的一项基于端口的安全技术。一般情况下，MAC 地址表是交换机根据所连接的网络设备，通过源地址学习自动建立起来，但网络管理员也可以手动在表中加入特定网络设备的 MAC 地址,使之与交换机的相应的端口绑定，被绑定后的网络设备只能通过绑定了的交换机端口访问交换机，这样就大大提高端口安全性。增加了为每个 VLAN 记录一张单独的 MAC 地址表，将 VLAN，端口，和 MAC 地址一对一,端口与 MAC 地址绑定后，只在对应的 VLAN 里有效。

将端口号和 MAC 地址绑定后，可以防止 ARP 欺骗

图片 5-55

Ø 绑定新的 MAC 地址

填写 MAC 地址，选中端口后，点击添加，则就可以在查看绑定的 MAC 地址条目中看到

5.5.7. MAC 地址过滤

MAC 地址过滤是交换机的另一项网络安全技术。用户可以自行把网络设备的属于该 VLAN 的 MAC 地址添加到 MAC 地址过滤表中，那过滤后的 MAC 地址，只在对应的 VLAN 中有效，被添加到 MAC 地址过滤表中的网络设备将无法访问交换机。此功能允许用户将 MAC 地址添加到过滤列表中，在过滤列表中的 MAC 地址将被交换机屏蔽

图片 5-56

在 MAC 地址里面填写要过滤的 MAC 地址，它即会出现在当前过滤的 MAC 地址表中

5.5.8. MAC 地址学习

此功能允许用户为每一个端口设置 MAC 地址学习的处理机制。Disable 某一个端口的 MAC 地址学习，动态 MAC 地址就不能被添加到表中。这样，除了静态 MAC 地址外，所有的未知源 MAC 包将被丢弃。

图片 5-57

Ø 查看 MAC 地址学习的端口号

每一个端口对应一个 MAC 地址学习状态

Ø MAC 地址学习

输入端口号以及 MAC 地址学习状态 enable 或 disable

5.5.9. MAC 地址老化

此功能允许用户设置 MAC 地址表的处理机制。一个空闲的 MAC 地址超过了 MAC 地址老化时间后，将会被 MAC 地址表移除。此处设置的时间对静态 MAC 地址是无效的

图片 5-58

Ø MAC 地址老化时间：

输入 MAC 地址老化时间，范围为 30-1000s。默认为 300 秒

5.6. QOS

传统的分组网络对所有报文都无区别的等同对待。每个交换机/路由器对所有的报文采用先入先出的策略FIFO处理，尽最大的努力Best-Effort将报文送到目的地，但对报文传送的延时、延时抖动等传输性能不提供任何承诺和保证。

随着计算机网络的高速发展，对带宽、延迟、抖动敏感的语音、图像、重要数据越来越多地在网上传输。这样一方面使得网上的业务资源极大地丰富，另一方面则由于经常遭遇网络拥塞，人们对网络传输的服务质量QoS Quality of Service提出了更高的要求。

以太网技术是当今被广泛使用的网络技术。目前，以太网不仅成为各种独立的局域网中的主导技术，许多以太网形式的局域网也成为了 Internet 的组成部分。而且随着以太网技术的不断发展，以太网接入方式也将成为广大普通 Internet 用户的主要接入方式之一。因此要实现端到端的全网 QoS 解决方案，不可避免地要考虑以太网上的 QoS 业务保证的问题。这就需要以太网交换设备应用以太网 QoS 技术，对不同类型的业务流提供不同等级的 QoS 保证。尤其是能够支持那些对延时和抖动要求较高的业务流。

QOS 包括：802.1p 队列映射、端口默认优先级、队列调度、信任模式。下面详细说明

5.6.1. 802.1p 队列映射

此功能将影响 VLAN 的优先级。基于 VLAN 的优先级 0-7，可以映射到交换机的 8 个队列 0-7。

图片 5-59

每一个优先级都可以选择队列 0-7。默认情况下，优先级 0、1 映射到队列 0，优先级 2、3 映射到队列 1，优先级 4、5 映射到队列 2，优先级 6、7 映射到队列 3

5.6.2. 端口默认优先级

图片 5-60

Ø 设置端口默认优先级：

输入端口号和优先级，则更改后的信息会在查看端口默认优先级里面出现

5.6.3. 队列调度

当网络拥塞时，必须解决多个报文同时竞争使用资源的问题。通常采用队列调度加以解决。这里介绍 2 种各具特色的队列调度算法：严格优先级 SP（Strict-Priority）队列调度算法加权轮循 WRR Weighted Round Robin 调度算法和带最大时延的 WRR 调度算法。

Ø SP调度算法（Always High）

SP 队列调度算法是针对关键业务型应用设计的关键业务有一重要的特点，即在拥塞发生时要求优先获得服务以减小响应的延迟。以端口有 8 个输出队列为例优先队列将端口的 8 个输出队列分成 8 类分别为高优先队列中优先队列正常优先队列和低优先队列（依次为 7~0 队列），它们的优先级依次降低。在队列调度时，SP 严格按照优先级从高到低的次序优先发送

较高优先级队列中的分组，当较高优先级队列为空时，再发送较低优先级队列中的分组。这样，将关键业务的分组放入较高优先级的队列，将非关键业务如 E-Mail 的分组放入较低优先级的队列，可以保证关键业务的分组被优先传送，非关键业务的分组在处理关键业务数据的空闲间隙被传送。

SP的缺点是拥塞发生时如果较高优先级队列中长时间有分组存在那么低优先级队列中的报文就会由于得不到服务而“饿死”。

Ø WRR调度算法

交换机的端口支持8个输出队列，WRR队列调度算法在队列之间进行轮流调度保证每个队列都得到一定的服务时间。WRR 队列还有一个优点是，虽然多个队列的调度是轮循进行的，但对每个队列不是固定地分配服务时间片——如果某个队列为空，那么马上换到下一个队列调度，这样带宽资源可以得到充分的利用。

当网络拥塞时，必须解决多个报文同时竞争使用资源的问题，通常采用队列调度加以解决。交换机依据报文的COS优先级进行入队列操作

严格优先级队列SQ保证高优先级业务总是在低优先级业务之前处理；WRR是一种加权循环队列调度机制，首先处理高优先级，但在处理高优先级业务时，较低优先级的业务并没有被完全阻塞，而是按一定的比例同时进行。NSW1924F允许严格优先级队列与加权循环队列同时存在。

队列调度可以按照这两种方法进行

Ø 根据权重的高低，来排列转发数据的先后，即 WRR

图片 5-61

Ø 永远执行最高优先级的，除非最高优先级没有数据了，才会往下面依次转发。在低优先级转发数据的时候，只要发现最高优先级又有数据了，那马上就又转发最高优先级的。即 Always High

5.6.4. 信任模式

图片 5-62

信任模式包括二层信任、三层信任和二三层同时信任。QoS 信任模式是针对报文协议头的。二层信任时，使用二层的协议头做为 QoS 的依据，如 IEEE 802.1p 优先级。三层信任时，使用三层的协议头做为 Qos 的依据，如 IP 包中的 DSCP。二三层协议头同时信任时，三层的 DSCP 优先。

5.7. 组播管理

组播管理包括：IGMP Snooping 和组播路由端口。下面分别详细说明

5.7.1. IGMP Snooping

IGMP 用来窥测 IP 多播组的状态，显示它的标记 VLAN 和未标记 VLAN 网络的相关信息。Enable IGMP snooping，可以监视到 IGMP Snooping 的信息，它包括多播组、VID 和端口

图片 5-63

Ø IGMP Snooping 状态：

如果你想开启 IGMP Snooping，则请选择 Enable，否则选择 Disable

5.7.2. 组播路由端口

图片 5-64

Ø 配置组播路由端口：

输入端口号和 VLAN ID，点击增加，则此信息出现在下方的“ 查看组播路由端口 ”，也可以删除。

5.8. 网络分析

网络分析包括：端口分析、端口镜像、QOS 统计器、防水墙日志、ARP 攻击日志。下面详细说明

5.8.1. 端口分析

此功能显示了端口的相关信息。一次只能够查询一个端口的信息

图片 5-65

在查看端口号里面输入要查看的端口号，则下方的查看端口分析即出现相关信息。例如查看端口 20 的分析结果如下

图片 5-66

5.8.2. 端口镜像

端口镜像提供端口监视功能，它把指定端口的数据包复制到监控端口。允许用户自行设置一个监视管理端口来监视被监视端口的数据。监视到的数据可以通过 PC 上安装的端口监视软件反映，如 EtherPeek NX、SpyNet 等，用户把监视到的数据进行分析就可以知道被监视端口情况，从而进行网络检测、监控和故障排除。

例如：设置端口 1 去监视从端口 5 出去数据到端口 6 进来的数据：

具体操作：在流量捕获配置下，“ 捕获状态 ”设置为“ Enable ”，“ 捕获端口 ”框选中“ Port1 ”，点击“ 确定 ”。然后在“ 被监视源端口列表 ”输入“ 5 ”，在“ 被监视目的端口列表 ”输入“ 6 ”，点击“ 增加 ”，查看捕获器中会显示配置的条件。

图片 5-67

Ø 流量捕获配置：

选择捕获端口和捕获状态。

Ø 镜像端口配置：

当流量捕获配置选择状态为 Disable 时，此项不可填写。当需要填写时，请填写被捕获源端口列表和被捕获目的端口列表

5.8.3. QOS 统计器

图片 5-68

此处显示在**安全－ACL** 输入的统计器所监测到的包个数

5.8.4. 防水墙日志

图片 5-69

此处显示**安全－网络防水墙**开启时监测到的防水墙日志

5.8.5. ARP 攻击日志

图片 5-70

此处显示 ARP 攻击的相关攻击信息，包括距离当前时间、端口号、攻击类型、攻击者 MAC、攻击者 IP 以及攻击次数

5.9. 网络设备保护

网络设备保护包括：主机安全保护、网络设备保护和应用程序优先级。下面详细说明

5.9.1. 主机安全保护

图片 5-71

图片 5-72

Ø 主机安全保护

² 安全策略：

包括：所有主机能访问网络、列表主机能访问网络和绑定主机能访问网络。

² 绑定策略：

包括只绑定 ARP 报文和绑定 ARP 和 IP 报文。

Ø 添加网络设备

分为自动搜索网络设备和手动添加网络设备。在选择自动搜索网络设备时，要填写起始/结束 IP 地址和 VLAN。在选择手动添加网络设备时，则需要填写 IP 地址、MAC 地址、VLAN、端口号，选择设备类型（主机/路由器/DHCP Server）和带宽限制。

Ø 查看网络设备属性

查询时需要填写设备 IP 和 VLAN

Ø 网络设备列表

在前面添加了网络设备后，此处会显示网络设备列表的信息。点击某一个条目，出现设备属性配置页面图片 5-73，请在此页面设置 MAC 地址、VLAN 号，端口号、设备名称、设备类型、路由器 IP（如果选择设备类型为“ 路由器 ”）和带宽限制

图片 5-73

在图片 5-72 中，点击批量限流，出现批量限流页面图片 5-74，请在此页面输入起始/结束 IP 地址、VLAN、路由器 IP 和带宽限制

图片 5-74

5.9.2. 网络设备保护

图片 5-75

Ø 启用主机<－>路由器带宽限制：

启用本功能将会对主机到路由器之间的速度进行限制，请首先配置主机带宽限制

Ø 启用 DHCP Server 保护功能：

本功能对合法 DHCP Server 进行保护，防止非法 DHCP Server 的干扰。请首先配置合法 DHCP Server（在**网络设备保护－主机安全保护**里面选择网络设备属性是 DHCP Server）

Ø 路由器端口速度限制：

在**网络设备保护－主机安全保护**里面选择网络设备属性是路由器时，这项功能方可使用

5.9.3. 应用程序优先级

根据设置的所需应用，来决定其处理级别的高低。

例：一般来说，如果遇到内网有人下载 BT，那是肯定会很快的把带宽给占满的，这样，就有可能影响内网的其他用户上网。甚至连 QQ 发送消息或者 QQ 语音都无法正常使用。那为了满足大部分用户的 QQ 使用，您就可以把它的优先级设置为高优先级，既转发数据的时候，优先转发关于 QQ 的。做到了就算有人使用 BT，对 QQ 一些简单的操作也不会受影响。

图片 5-76

Ø 程序优先级模板应用

² 应用程序模板：

请选择常见的应用程序

² 优先级：

为选择的应用程序设置优先级。包括高优先级、中优先级和低优先级

Ø 用户定义应用程序优先级

由于应用程序不一定全部在应用程序模板中出现，所以在应用程序模板中找不到想要的应用程序时，就需要自定义。填写应用程序的名称、协议、端口，然后为它选择优先级。填写完成，点击确定后，此内容即会出现在“ 查看程序优先级应用 ”里面。

5.10. 单 IP 管理

图片 5-77

显示当前模式、管理模式、IPSTACK 组、系统优先级、IPSTACK MAC 以及 IPSTACK 名称的信息。您可以对 IPSTACK 名称进行修改

如果您的网络中有多台交换机，则此时您就可以用模式为“ 管理交换机 ”的交换机来管理所有的交换机来实现整网联动管理，而不需要一一登录其他的交换机，

6. CONSOLE 控制台

除了 WEB 管理，您也可以通过使用例如 Microsoft Windows 的超级终端对交换机进行管理和配置。这种方式可以方便地通过 PC 的串行口对设备进行管理，由于该方式不依赖于网络连接，所以当出现链路故障时，通常使用这种方式进行检测。请注意 CONSOLE 口在交换机的后面板处

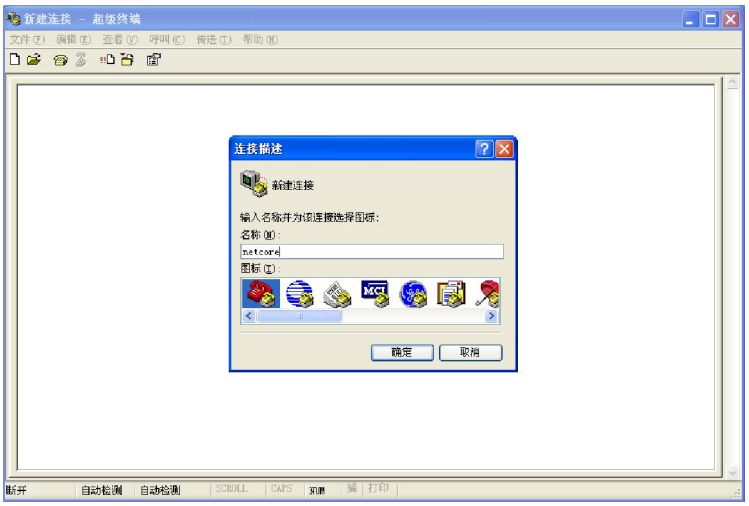
注：此 CONSOLE 管理只用于 X-MODE 升级和恢复默认参数

6.1. 恢复默认

1、连接计算机和交换机串口，点击**程序－附件－通讯－超级终端**，打开超级终端

图片 6-1

2、输入超级终端名称，点击确定



图片 6-2

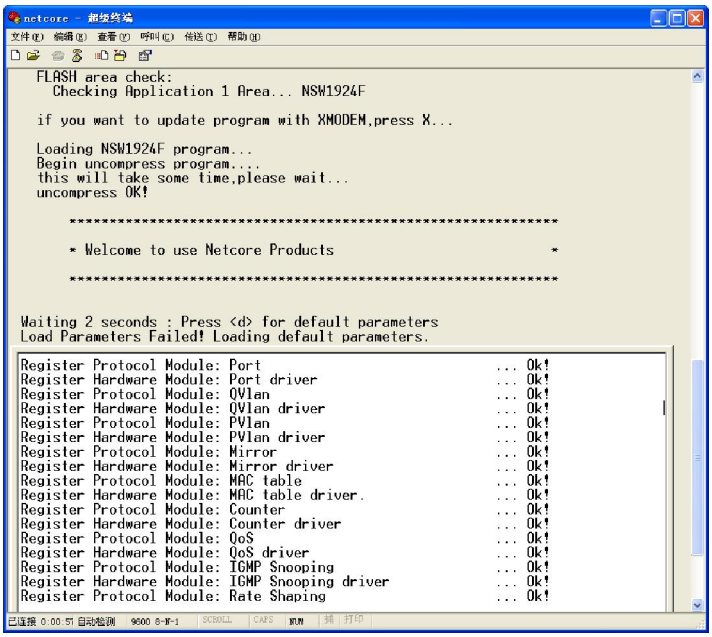
3、选择连接时使用的端口，点击确定

图片 6-3

4、参照下图设置串口属性，点击确定

图片 6-4

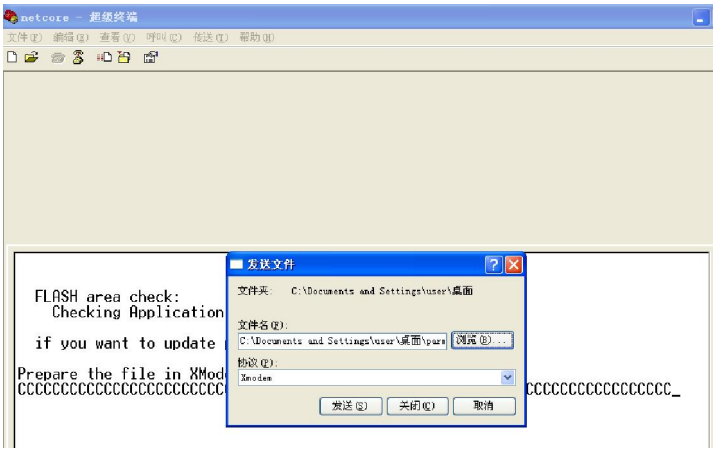
5、将 NSW1924F 通电，此时按住键盘上“ D ”不放，恢复成功后超级终端窗口内会显示恢复默认的信息，恢复成功，如下图



图片 6-5

6.2. X-MODE 升级

请参照恢复默认步骤 1－4 启动超级终端，此时按住键盘“ X ”不放，待出现 Prepare the file in XModem 字样，选择菜单栏传送功能，在弹出窗口中选择欲发送文件路径，选择协议 Xmodem，点击发送。



图片 6-6

待超级终端界面出现升级完成提示后，断电重启交换机，升级成功。

```
  FLASH area check:
    Checking Application 1 Area... NSW1924F

  if you want to update program with XMODEM,press X...

Prepare the file in XModem client.
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
modem received ok.
md5 check OK.write flash.
update complete! Reset your device.
Reset Your System.
```

图片 6-7

7. 疑难解答

1、链路状态指示灯显示不正常（Link-Error）

Ø 查看链路另一端是否良好地连接到 PC 网卡或其他以太接口上；

Ø 检查连接电缆及两端的 RJ45 接头是否有锈蚀或损坏；

Ø 使用 WEB 方式(检查该端口的通讯配置（双工、速度），确定其配置是否与链路另一端相匹配。

注意：当链路两端均强制设置双工和速度时，如果设置不匹配，是无法建立连接的。

2、链路状态指示灯显示正常但无法通讯

出现这种情况时，请按照下列步骤进行检查：

Ø 使用 WEB 方式（见端口状态查询）检查该端口是否被停止，如果显示该端口被停用，则使用 WEB 方式（见端口配置中的关闭/打开）打开该端口；

Ø 使用 WEB 方式检查该端口是否在 VLAN 设置中与其他端口隔离；端口只能和同一个 VLAN 内的成员端口进行通讯。

3、无法远程登录管理交换机

请按照下面的步骤对 NSW1924F 进行检查：

Ø 检查 NSW1924F 是否成功启动；

Ø 检查有无链路故障；

Ø 使用 PING 程序检测 NSW1924F 有无回应：如果没有回应，则检查 NSW1924F 和 PC 的 IP 地址配置是否正确；如果有回应，则可根据 HTTP 连接反馈信息来判断故障原因。

检查 IP 地址设置，请按照下面的步骤对 NSW1924F 进行检查：

Ø 检查 PC 的 IP 地址、子网掩码以及默认网关设置是否是你期望的设置：在 Windows 命令行方式下输入 ipconfig 查看 PC 的 IP 地址配置；

Ø 检查 NSW1924F 的 IP 地址、子网掩码以及默认网关设置是否是你期望的设置：在 CONSOLE 方式下使用检查 NSW1924F 的 IP 地址设置；

Ø 检查 PC 和 NSW1924F 的 IP 地址是否被其它设备占用；

检查远程登录帐号

Ø 用户使用 WEB 方式远程登录时，如果 NSW1924F 连续要求输入帐号和密码，这可能是输入的帐号不存在或输入的密码错误。

4、交换机启动故障

如果不能从 CONSOLE 端口连接的终端屏幕上观察到交换机成功启动，请按下列步骤检查：

Ø 检查所使用的终端软件设定的串口号是否正确 通常 PC 上带有 2 个串口，分别是 COM1

和 COM2；

- Ø 检查所使用的终端软件的通讯配置是否是：9600bps、8 数据位、1 停止位、无奇偶校验、无流控；
- Ø 检查 PC 上的串行口工作是否正常：可以使用串口鼠标来检测串口硬件有没有故障；
- Ø 确认用户的 Windows 操作系统中有没有其他程序在使用该串口；Windows 操作系统不允许多个程序同时使用一个串口

5、电源故障

首先查看交换机的电源指示灯，如果指示灯熄灭，可能是外电源连接不良，请确定电源接线板供电是否正常，并检查电源线与电源接线板、以及与 NSW1924F 的连接是否稳定可靠。