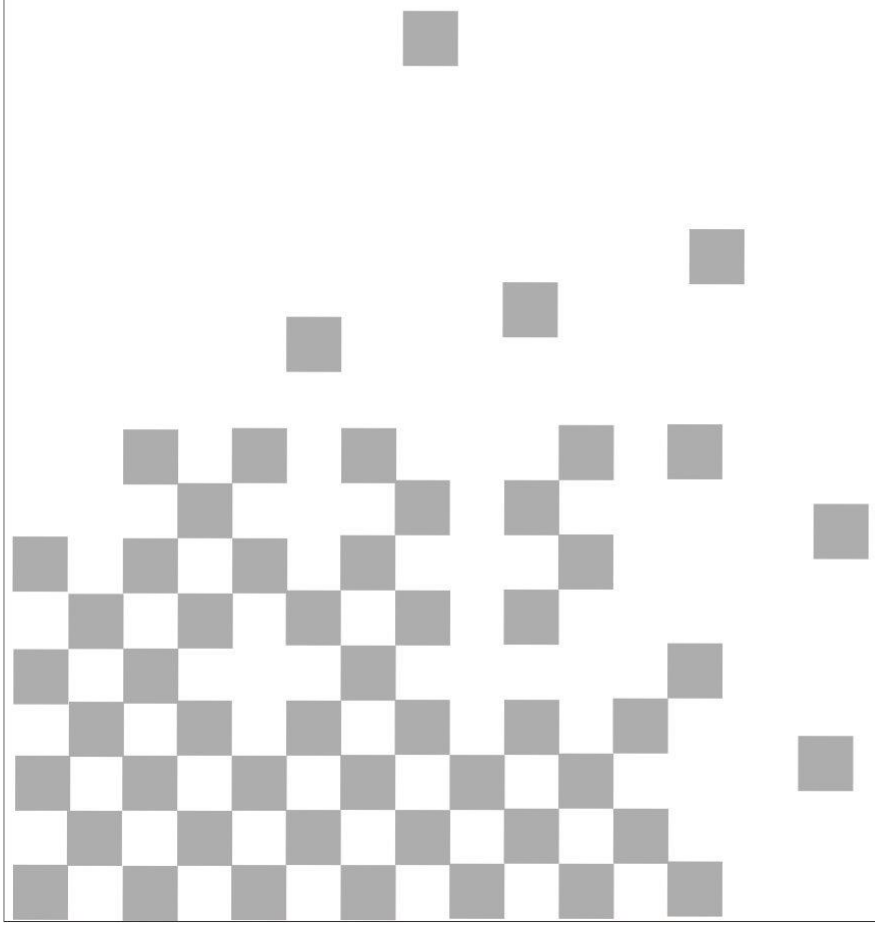
net·core 磊科®

NSW1824C/NSW1824CF

千兆安全型交换机

用　户　手　册



A 类设备声明

此为 A 级产品，在生活环境中，该产品可能会造成无线电干扰，在这种情况下，可能需要用户对其干扰采取切实可行的保护措施

版权声明

认证

通过 FCC、CCC 认证

手册说明

本手册旨在帮助您正确使用这款交换机，请在安装交换机前，详细阅读本手册。

：该图标名为“注意标”，表示某些功能设置要格外小心，如果设置错误可能导致数据丢失或是网络不通。

：该图标名为“提示标”，表示问题的补充说明。

提示

本手册的用途只限于磊科 24、48 口全千兆二+四层系列交换机，请以实际机型为参照进行下载。本说明书中出现的产品图片以及相关信息如无详细说明一律以 NSW1824CF 交换机为例。

包装清单

- 一台 NSW1824CF
- 一张 CD
- 一本安装指南
- 一根串口线
- 一根电源线
- 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。

安装之前

首先非常感谢您选用著名网络设备厂商 Netcore24 口千兆安全型接入层交换机。

在使用交换机之前，请仔细阅读本指南以便快速完成安装。如有疑问请拨打磊科免长途技术支持热线 400-810-1616，我们的技术支持工程师将为您做详细解答。

目录

1. 简介

1.1. 产品概述

NSW1824CF 千兆安全型交换机专为连接中小型网吧及企业接入层设计。完全兼容 IEEE802.3 10Base-T 以太网协议，IEEE802.3u 100Base-TX 快速以太网协议以及 IEEE802.3ab 1000Base-T 千兆以太网协议

NSW1824CF 千兆安全型交换机提供 24 个千兆铜缆口，采用 19 寸标准机架式设计，属于磊科联动网管系列产品，拥有单 IP 管理功能，并且可以支持网刻分流，无盘加速，以及新一代全自动 ARP 绑定技术。是做全千兆网吧的不二之选。

NSW1824CF 千兆安全型交换机提供中文 WEB 页面管理方式及软件升级方式。最大限度的提高了人机交互质量。相信选用这一款功能强大的磊科 NSW1824CF 是您明智的选择！

1.2. 主要特性

- 支持整网联动管理
- 支持无盘加速
- 支持网刻分流
- 支持游戏加速
- 支持链路聚合
- 支持 802.1Q VLAN
- 支持 ARP 自动绑定
- 支持端口镜像
- 支持基于 WEB 的管理
- 支持串口方式下的管理配置（仅限于恢复默认参数和升级）
- 支持基于 WEB 方式的固件升级
- 支持基于 X-Modem 的固件升级
- 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

- 遵循 IEEE802.3 10BASE-T Ethernet 标准

- 遵循 IEEE802.3u 100BASE-TX　Fast Ethernet 标准
- 遵循 IEEE802.3ab 1000BASE-TX　Giga Ethernet 标准

1.4. 工作环境

温度

- 0 °to 40 °C（运行）
- -20 °to 70 °C（储存）

湿度

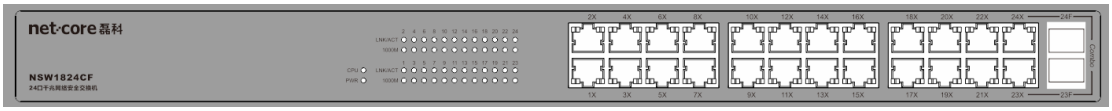
- 10% to 90 %无凝结（运行）
- 5% to 90%无凝结（储存）

电源

- 100-240V AC，50-60HZ
- 产品外观

1.4.1. 前面板

NSW1824CF 前面板由 24 个 10/100/1000M 自适应双绞线端口加 2 个光铜互用 Combo 口组成，以及相关 LED 指示灯组成，如下图所示：



图片 1-1

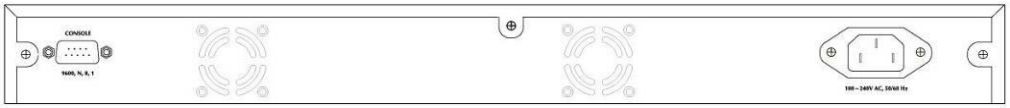
24个端口支持10Mbps、100Mbps 或1000Mbps 带宽的连接设备，均具有自动协商能力。每个端口对应有一组指示灯，即LINK/ACT 和1000Mbps 指示灯。

指示灯：

LED 指示灯	状态	功能
PWR	常亮	已通电
	常灭	未通电
CPU	常亮	系统工作正常
	常灭	系统异常
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	对应端口工作在 10M/100M 模式

1.4.2. 后面板



图片 1-2

- CONSOLE：CONSOLE 端口可用于恢复出厂设置（波特率：9600，数据位：8，停止位：1）及 Xmodem 升级。
- 电源：电源适配器插槽。

2. 硬件安装

2.1. 安装前的准备

- 放置交换机的表面必须至少能承重 4kg
- 供电的电源插座距离交换机须在 1.8 米之内
- 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
- 保证交换机的四周可以良好的通风散热
- 请勿将重物放置在交换机上

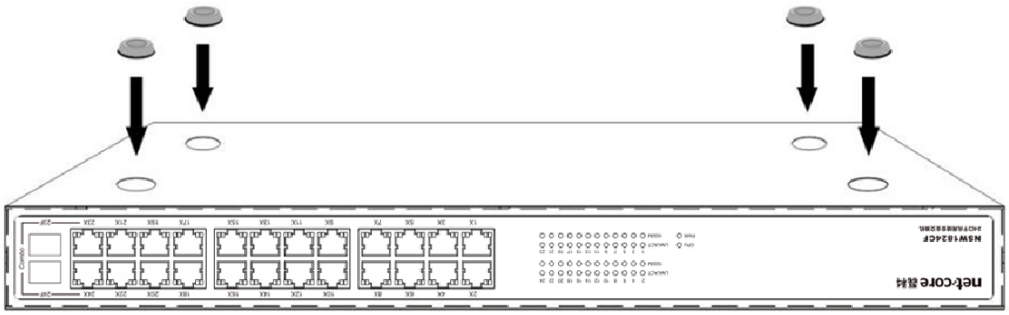
2.2. 桌面安装过程

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。

2.3. 机架安装过程

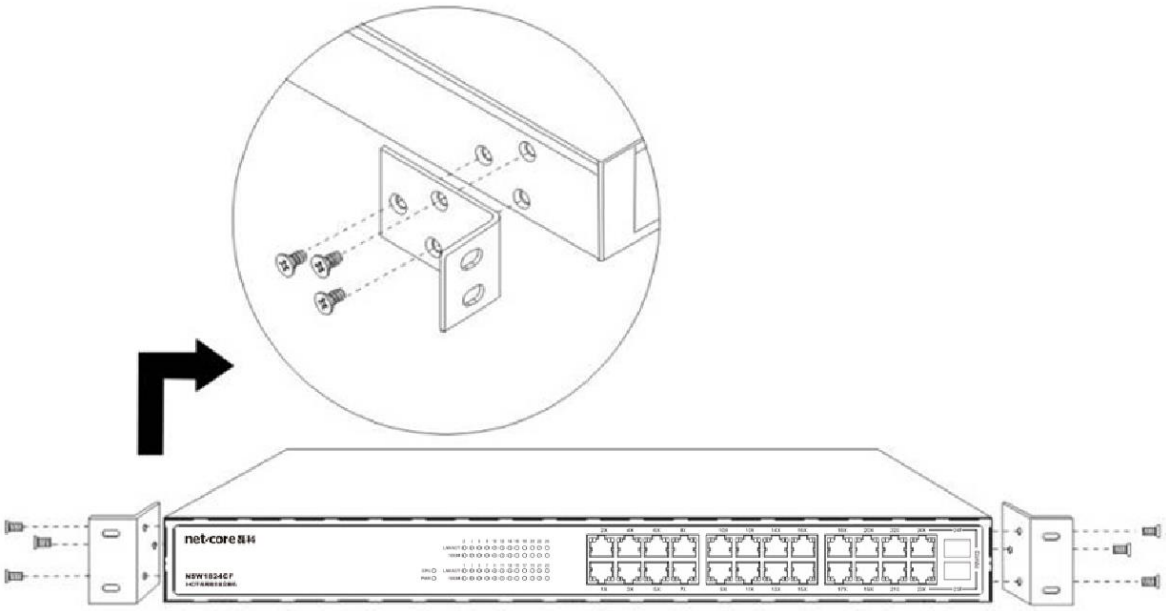
首先，需要将包装箱内已提供的上机架的配件用与其配套的螺丝固定在交换机的前面板的两侧，然后，再用螺丝将交换机安装在 19 英寸的机架内。

A:安装防滑脚垫。



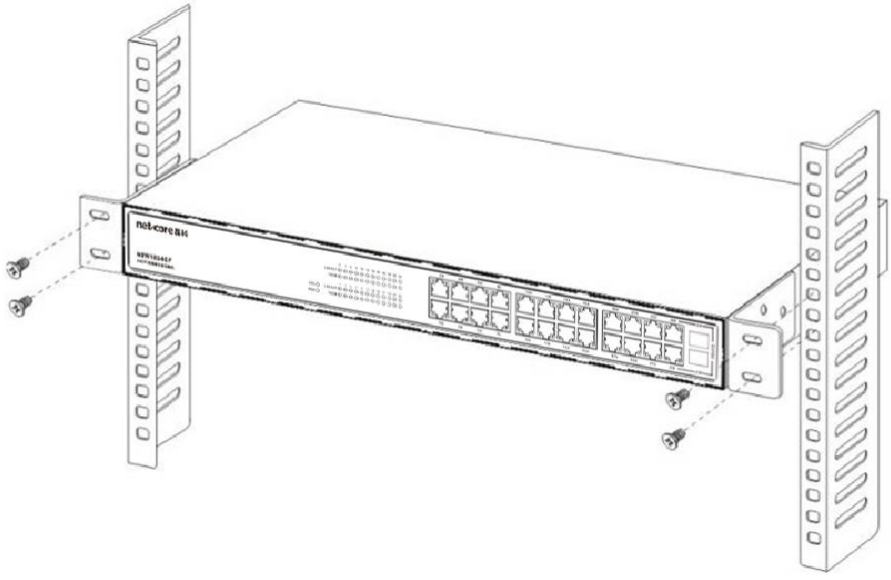
图片 2-1

B:安装交换机两侧耳片。



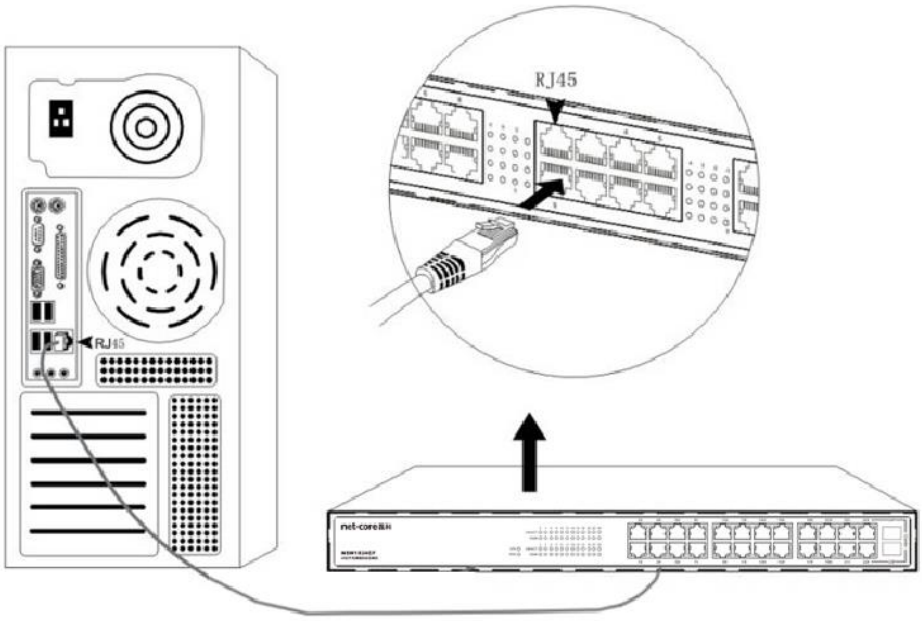
图片 2-2

C:上机架



图片 2-3

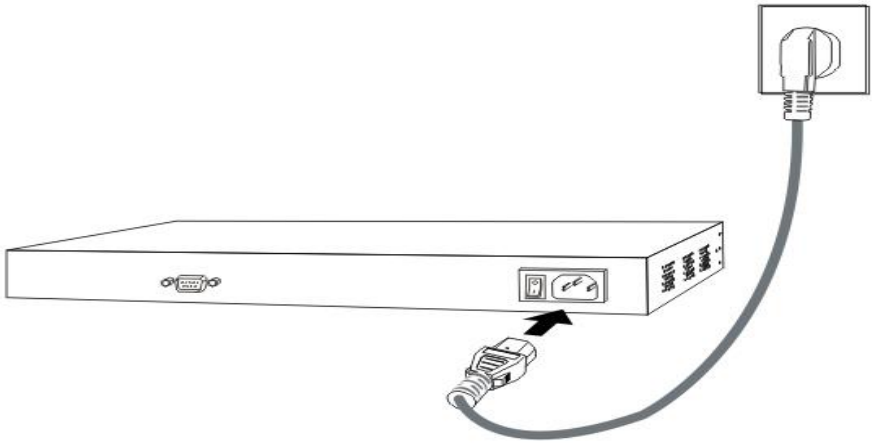
D:联机检查



图片 2-4

2.4.电源

交换机的输入电压范围是 100-240V AC（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。



图片 2-5

2.5. 注意事项

线缆长度

- 本设备与其它 IEEE802.3 兼容网络设备连接时，线缆长度应该符合双绞线组网标准

线缆类型及线序

- 设备在 3/4/5 类线缆上均可达到 10M 传输速率，若要使网络工作在 100/1000Mbps 的传输速率下，必须使用非屏蔽 5 类双绞线（UTP）或更高级别的线缆，若长期使用 3 或 4 类线缆将导致数据丢失
- 本设备的每个端口均具有自动线序交叉功能，可以使用任意线缆（平行线和交叉线）与其他网络设备相连

3. 登录

你可以通过基于 web 浏览器的配置来管理 NSW1824CF。要通过 web 浏览器配置 NSW1824CF，至少要有一台合理配置的电脑，通过以太网连接到 NSW1824CF。NSW1824CF 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

3.1. 配置电脑

3.1.1. 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。

4、选择 TCP/IP。点击属性。出现 TCP/IP 属性对话框

5、选择设置静态 IP 地址，输入 IP 地址为 192.168.2.***(1<***<255，且***不等于 11)

6、从 WINS 的配置对话框，确保设置了禁用 WINS 解析

7、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

8、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

9、点击确定，返回网络配置对话框

10、点击确定，如果想立刻重启，点击“是”

3.1.2. 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 3-1

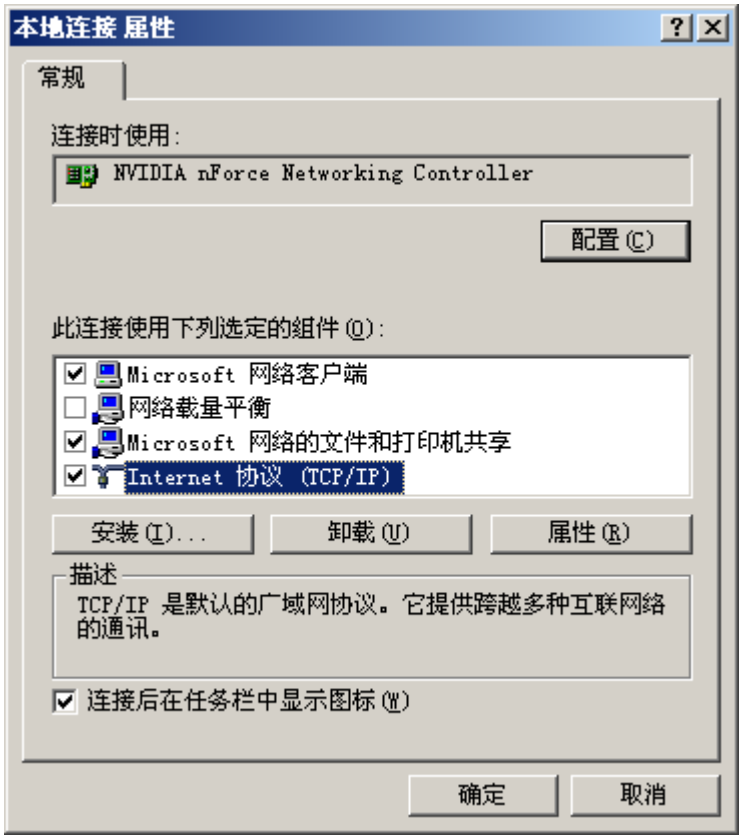
2、双击**网络和拨号连接**

图片 3-2

3、点击**本地连接**，右键选择**属性**

图片 3-3

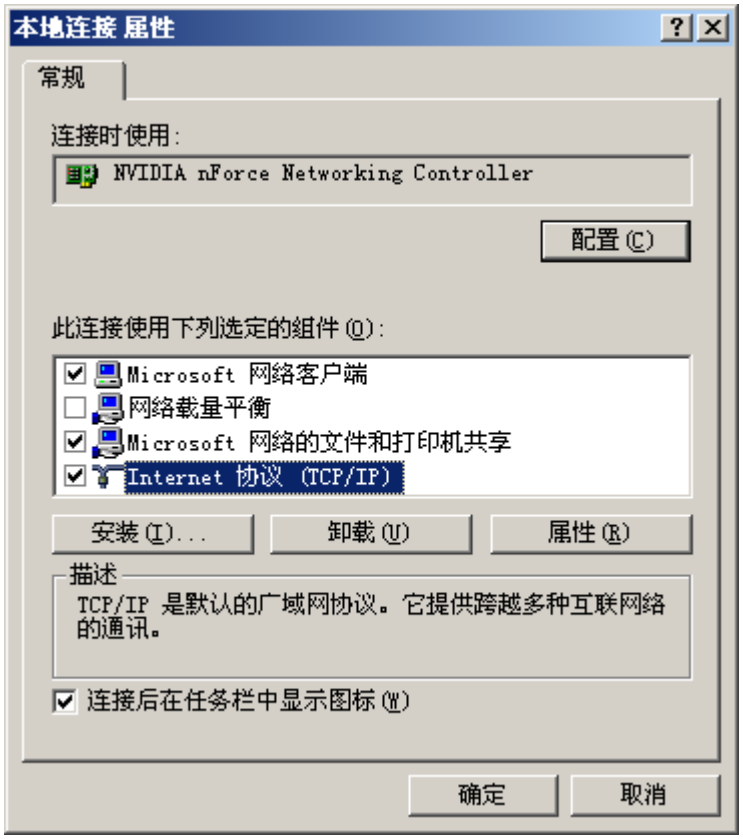
4、点击 **Internet 协议（TCP/IP）**，点击**属性**按钮



图片 3-4

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 3-5

3.1.3. 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 3-6

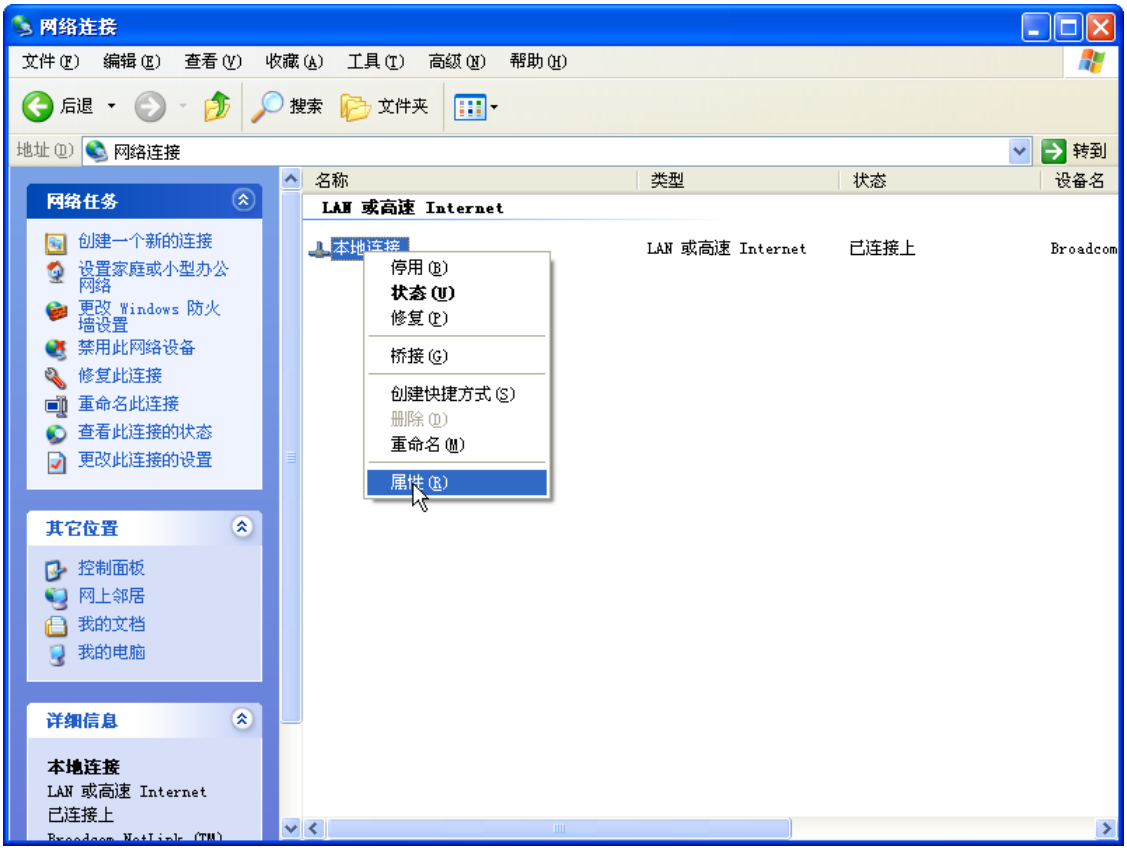
2、点击**网络和 Internet 连接**

图片 3-7

3、点击**网络连接**

图片 3-8

4、点击**本地连接**，右键点击**属性**

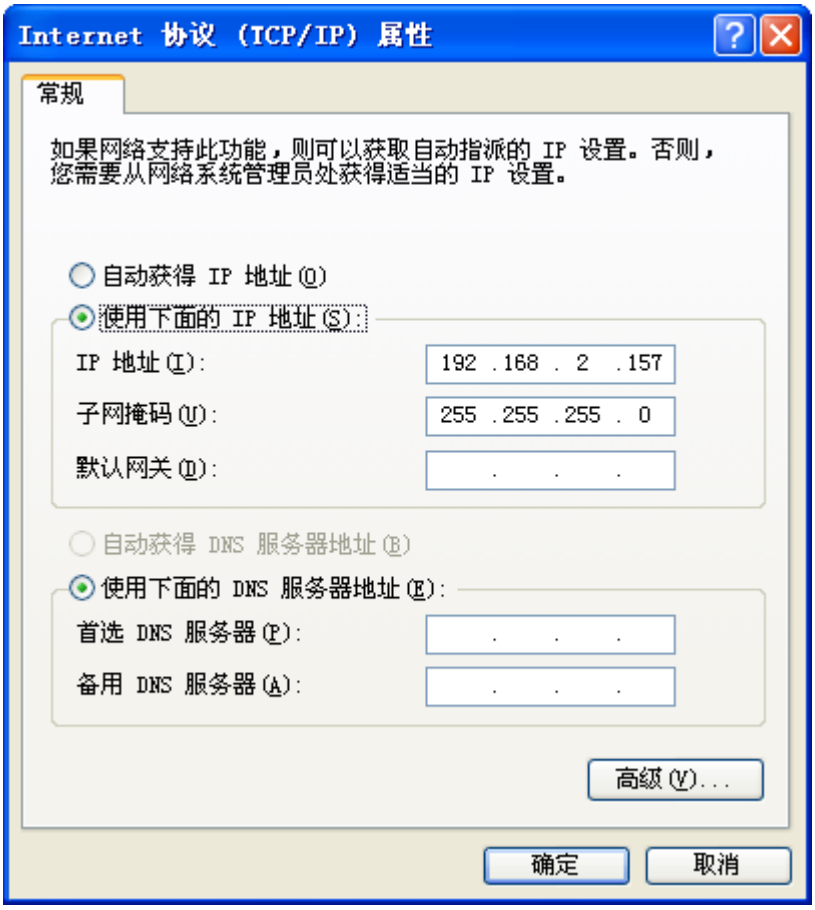


图片 3-9

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

图片 3-10

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**此交换机默认的 IP 地址为 192.168.2.11**)，**子网掩码 255.255.255.0**，默认网关和首选 DNS 服务器可不填然后点击确定，关闭 **Internet 协议（TCP/IP）属性**窗口



图片 3-11

7、点击**确定**，关闭**本地连接属性**窗口

图片 3-12

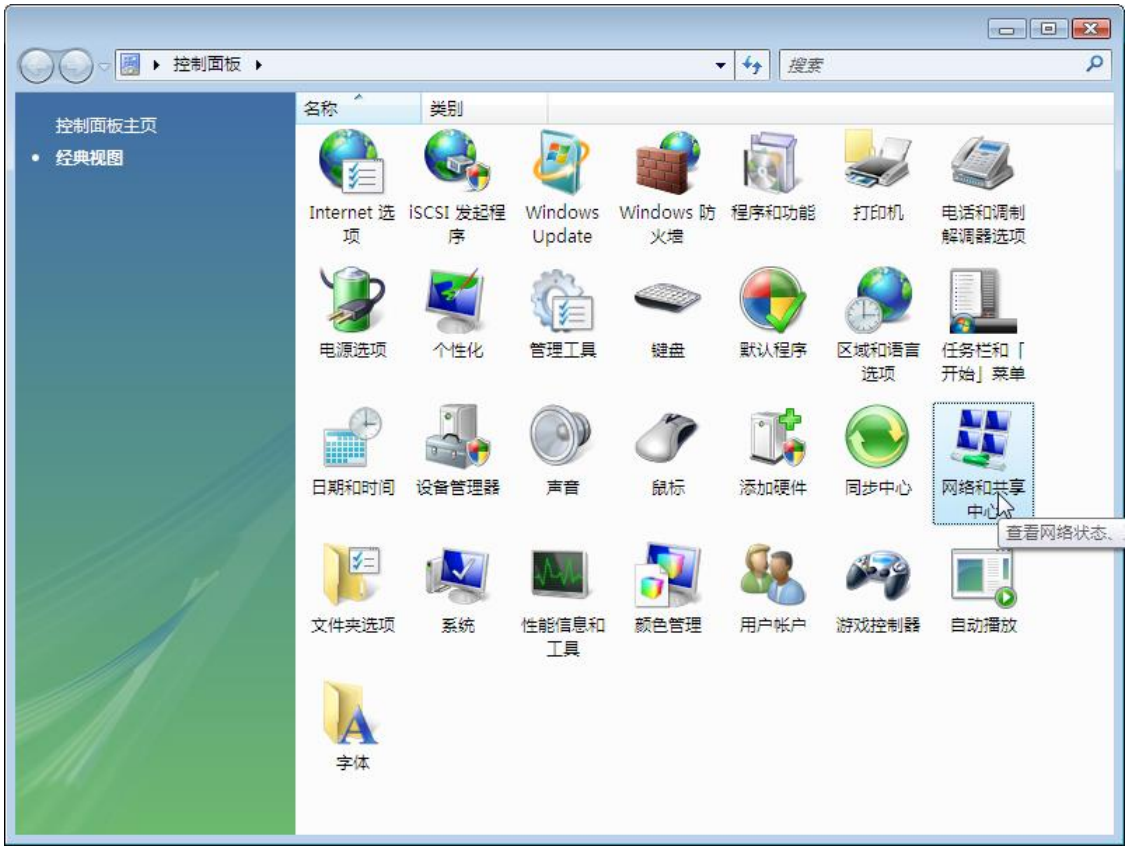
3.1.4. Windows Vista

请按照下述步骤配置你的电脑

1、**开始－控制面板**

图片 3-13

2、点击**网络和共享中心**

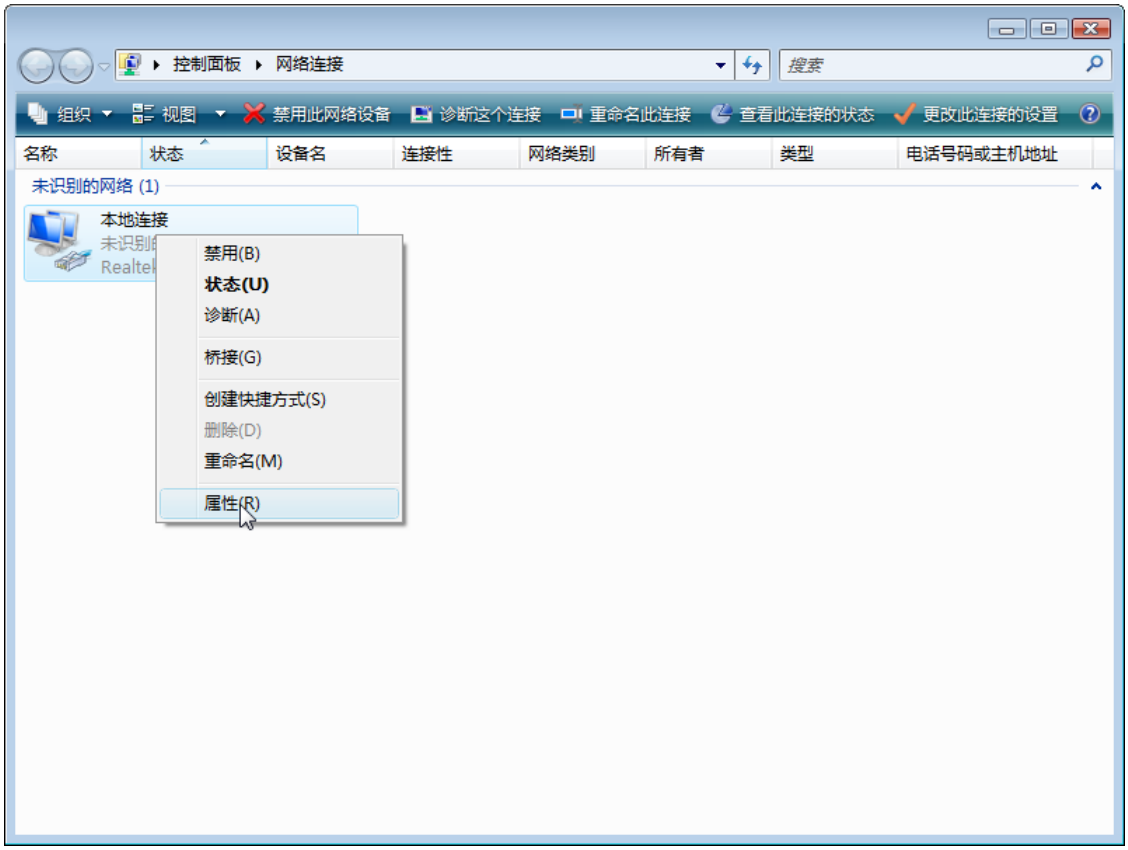


图片 3-14

3、点击**管理网络连接**

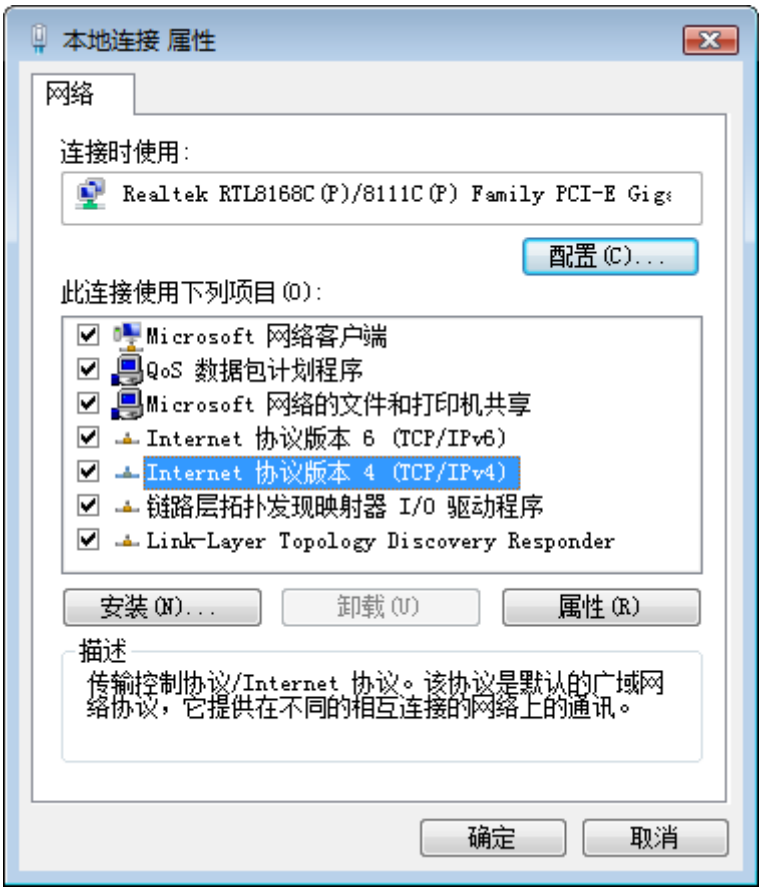
图片 3-15

4、右键点击**本地连接**，点击**属性**



图片 3-16

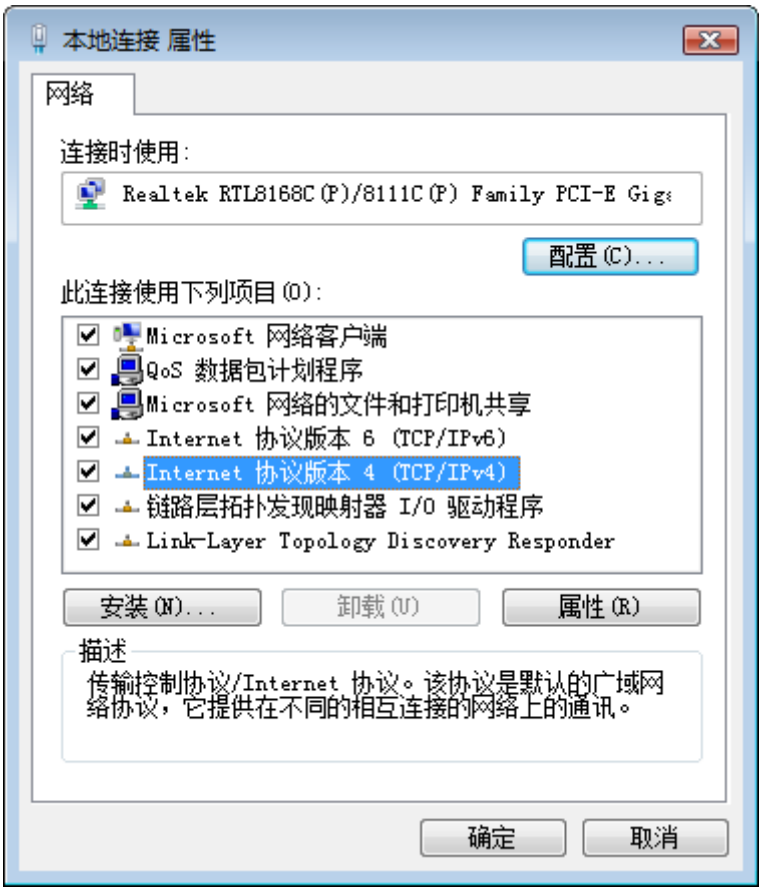
5、点击 **Internet 协议版本 4（TCP/IP）**，然后点击**属性**按钮



图片 3-17

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 3-18

3.2. 检查连接

设置完 TCP/IP 协议后，用 Ping 命令来验证电脑是否可以与 NSW1824CF 通信。要执行 Ping 命令，打开 DOS 窗口，在 DOS 提示里 Ping NSW1824CF 的 IP 地址

- 对 Windows 98/Me，开始－运行。输入 command 然后点击确定
- 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 NSW1824CF 和电脑之间的连接就成功的建立了

如果电脑没能连接上 NSW1824CF，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),
```

这时请确认您电脑的网络设置是否正确，网线是否完好。

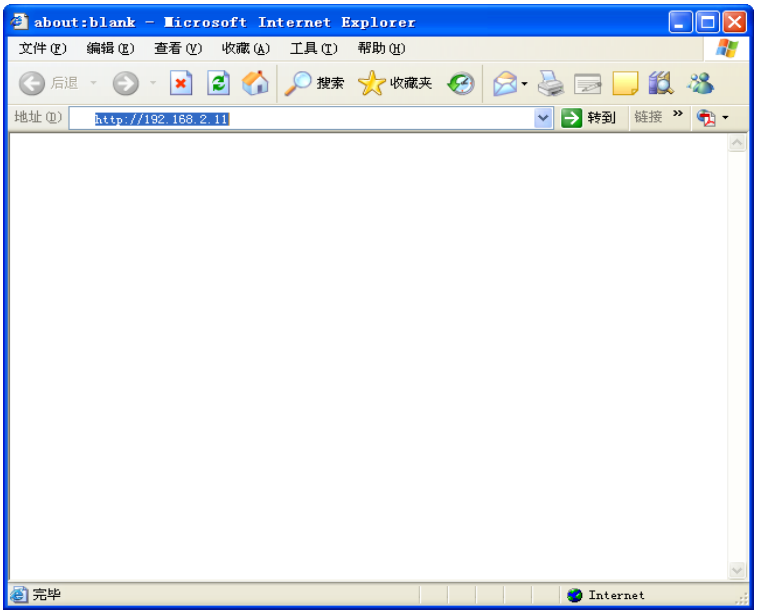
为了使整个网络运行成功，有必要通过安装了 WEB 浏览器的电脑设置 NSW1824CF。请按照以下步骤设置。

 注意：

在输入以上命令前需用一根 6 类双绞线将您电脑的网卡与交换机其中任意一个端口连接起来。

3.3. 登录

1、打开 IE 浏览器，在地址栏输入 http://192.168.2.11，后回车。



图片 3-19

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

图片 3-20

成功登录后，您就可以看到 NSW1824CF 的 web 设置页面

图片 3-21

3.4. 功能概述

NSW1824CF交换机功能丰富，包括系统管理、端口管理、冗余与备份、安全、联动管理等功能，本手册将在以下章节中分别为您介绍。

4. 配置指南

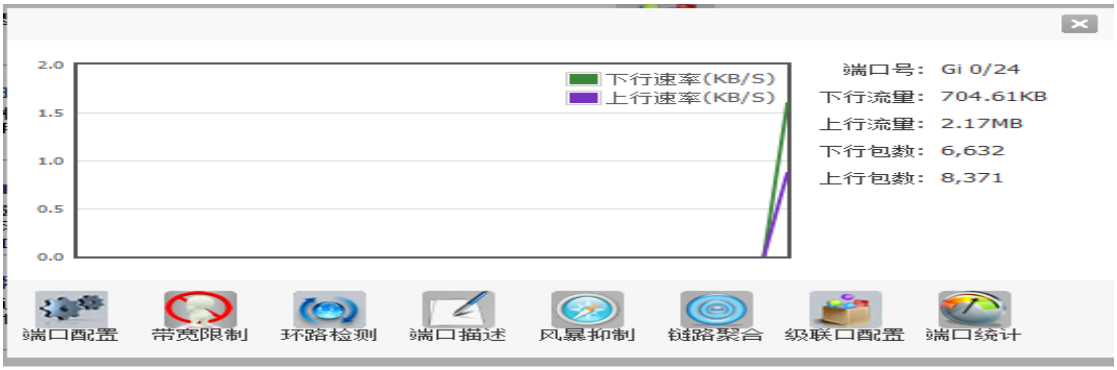
4.1. 首页

当您成功登录后，您就可以看到此交换机的首页。首页显示了该交换机系统的基本信息。

图片 4-1

- 管理页面上方区域：此处显示了此交换机的前面板。在前面板上，当前连接的端口指示灯显示为绿色，未连接的端口指示灯灰显。如图片 4-1 所示
- 管理页面下方区域区：此处显示交换机系统的系统菜单及特色功能展示。

提示：当交换机某一端口建立物理连接时，管理界面上方区域的前铭板对应的端口会显示插有网线，点击此图，会显示该端口的当前连接状态。下图为查看某一连接中的端口状态信息图：



图片 4-2

4.2. 系统管理

点击“系统管理”将得到如图片 4-3 所示：通过该项可以设置交换机的基本信息，主要包括：系统信息、IP 地址、修改密码、MAC 地址、管理 VLAN、CONSOLE 信息、系统时间设置、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

图片 4-3

4.2.1. 系统信息

图片 4-4

此处显示交换机系统的基本信息主要包括型号、MAC 地址、软件版本号、系统时间、CPU 占有率、内存占用率等信息。

4.2.2. IP 地址

图片 4-5

在此页面您可以设置 IP 地址、子网掩码、网关。**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。

4.2.3. 修改密码

图片 4-6

为交换机设置管理权限。

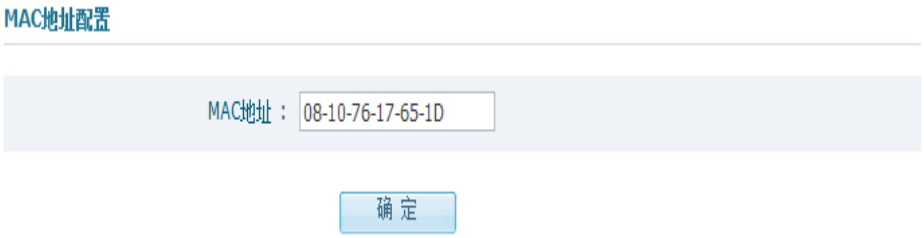
在首次使用交换机时，为了安全起见，请在此修改密码。修改完密码后，保存参数并重启交换机，下次登录时，请使用新密码。默认密码是 **guest**。

注意：

修改密码后请记录后新密码。如果密码忘记，将只有通过恢复出厂设置的办法为找回，但同

时交换机当前所配置的所有参数将丢失。

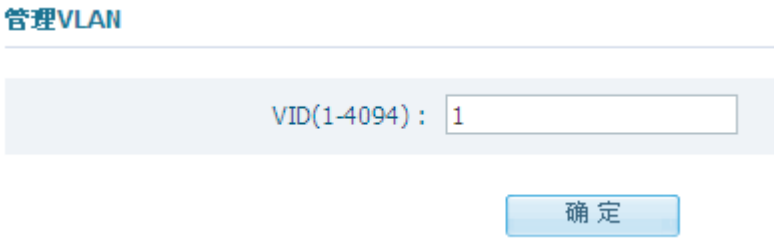
4.2.4. MAC 地址



图片 4-7

此处显示此交换机的硬件地址。您也可以修改这个值

4.2.5. 管理 VLAN

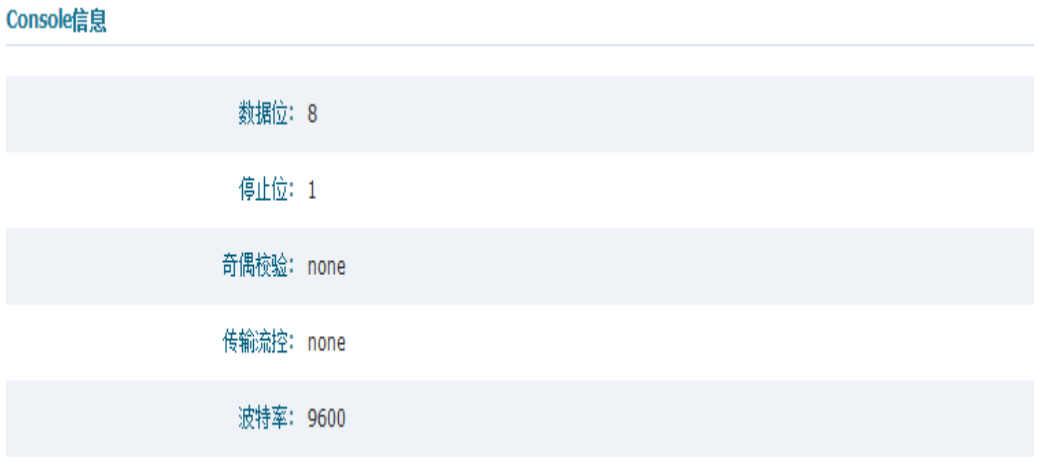


图片 4-8

VID，即 VLAN ID，您可以输入 1-4094 之间的数字。这是一种安全措施，通过管理 VLAN 的限制可以控制那些 VLAN 用户可以登录交换机进行配置。默认 1 VLAN 可以登录交换机进行配置。

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

4.2.6. CONSOLE 信息



图片 4-9

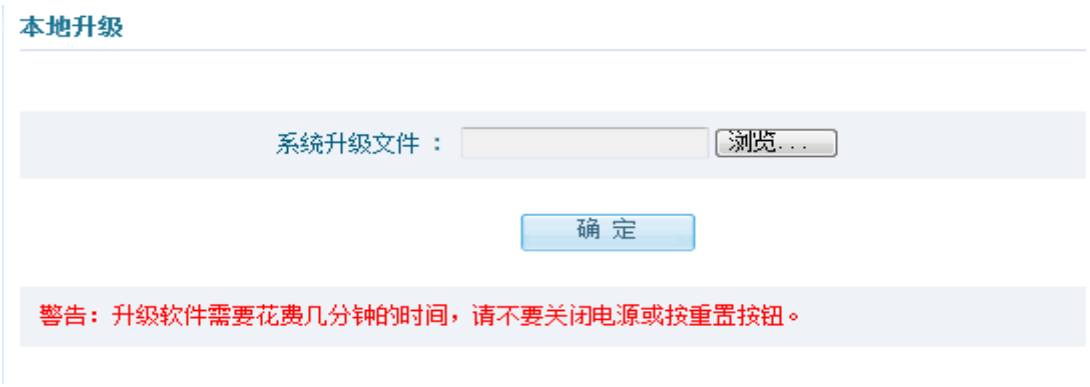
此页面显示 console 口（串口）信息。

4.2.7. 系统时间配置

图片 4-10

系统时间配置即 NTP 服务，可以使您的交换机自动连接远程 NTP 服务器来更新系统时间，默认为关闭状态。

4.2.8. 系统升级

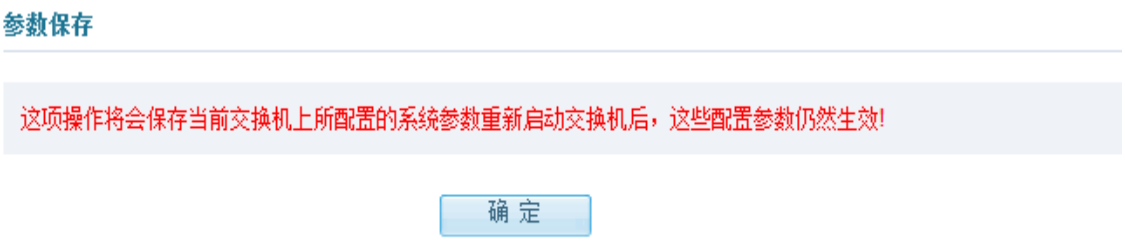


图片 4-11

通过该功能可以在本地对此交换机进行升级，当发现该款交换机软件较旧时请到我们的官方网站 www.netcoretec.com 相关页面下载相应较新软件后，再点击“浏览”按钮找到您下载到本地的升级软件；点击“开始升级”按钮执行软件升级；软件升级后交换机将自动重启。

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。

4.2.9. 参数保存



图片 4-12

通过该功能可以将当前所有配置进行保存。就算是交换机重启这些参数也不会丢失。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，交换机重启或断电后这些配置将全部丢弃。

提示：操作完某项操作后请及时保存参数，以避免不必要的麻烦。

4.2.10. 参数备份与恢复

图片 4-13

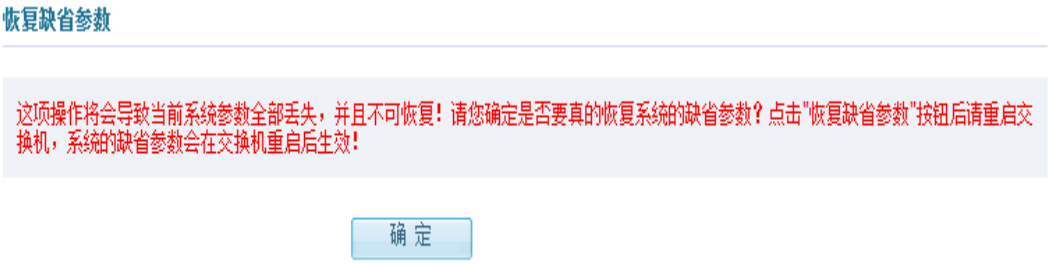
通过该功能可以将当前所有参数配置以文件的形式进行保存到您的本地硬盘上，一般是在交换机系统运行比较稳定时执行该功能。必要时您可以使用这个文件来恢复交换机系统。

- 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，按提示操作会保存一个文件到您的电脑。
- 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

提示：

在用备份文件恢复交换机系统前，建议先按 4.2.11 的方法把交换机恢复到出厂设置后再执行参数恢复操作，可避免不必要的麻烦。

4.2.11. 恢复缺省参数



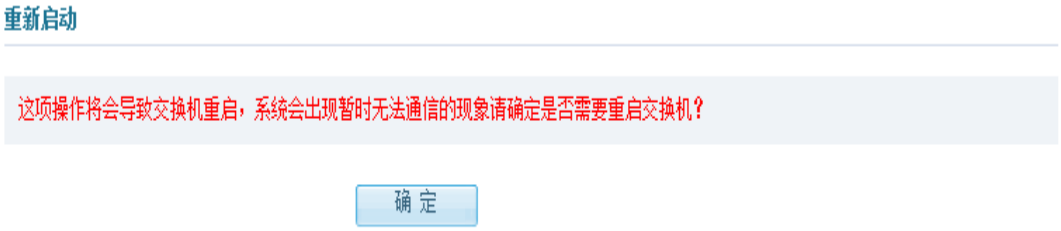
图片 4-4

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使用。

4.2.12. 重新启动



图片 4-5

点击“重新启动”，则交换机自动重启。

注意：

如果交换机没有做参数保存，执行该项操作后交换机当前所配置参数将丢失。

4.3. 端口管理

通过该项功能可以对交换机的端口进行基本配置。主要包括端口配置、端口统计、端口带宽限制、级联口配置、缓存调度策略、端口描述、端口风暴抑制等操作，下面将对每一个子项分别详细说明。

4.3.1. 端口配置

如图片 4-6 所示本项可以对交换机所有端口指定其工作速度及流控。同时也显示所有端口当前状况。

图片 4-6

- 查看端口状态
  - 管理状态：有 enable 和 disable 两种状态，可以在端口配置里面更改。
  - 连接状态：有 down 和 up 两种状态。其中 down 是端口未连接，up 是端口已连接状态。
  - 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。
  - 流量控制：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，流量控制是为了同步接收方和发送方的速度而进行的控制，当交换机上的转发缓冲区被占满后，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。缺省情况下，端口流控处于关闭状态。

注意：

- 端口配置项建议使用默认配置如不必要请勿修改。
- 流量控制功能慎用。特别是在大流量流且突发流（网克、无盘）时可能会导致网速变慢。

4.3.2. 端口统计

图片 4-7

显示当前交换机所有端口工作状态。主要包括接收包总字节、发关包总字节、接收包数及发送包数等信息。

- 点击刷新，可以显示此刻的端口统计信息。
- 点击“复位统计信息”，则发送、接收包数等信息被清空。

4.3.3. 端口带宽限制

无论您是哪种接入方式，您都需要合理的整体规划您的带宽，以保证您的带宽最大程度的优化和利用。可限制端口数为 24 个，限制带宽大小为 1000Kbps—1000000Kbps。该项功能是一种安全防御措施，在一个稳定的网络环境当中，只有当网络出现病毒或是攻击时才会大量出现这种无用报文。造成链路拥塞从而影响其它应用。如果这时做了端口带宽限制，那么交换机就会对入口和出口报文种类与速率进行监测，丢弃无用报文避免链路拥塞。

图片 4-8

提示：

- 如果您正在进行网克请不要设置端口带宽限制。
- 入口：即交换机端口接收，出口：即交换机端口发送。
- 此处带宽限制的单位是小“b”请注意区分。
- 出口带宽限制是针对端口下所有报文请慎用。如设置值太低，可能会导致全网网速慢。

4.3.4. 级联口配置

图片 4-9

交换机级联就是交换机与交换机之间通过交换端口进行扩展，一方面解决了单一交换机端口数不足的问题，另一方面也解决离机房较远距离的客户端和网络设备的连接问题。合理的设置交换机级联口有助于网速的提升。

图片 4-9 中桥接端口列表：显示交换机所有端口。

图片 4-9 中级联口列表：显示当前已处于级联的端口。

提示：

- 一般能设为级联口的端口为路由器所接端口、服务器所接端口以及下游交换机设置等。

- 如果需要使用主机安全绑定，请先不要配置级联口，以免搜不到主机 IP 地址之

4.3.5. 缓存调度策略

图片 4-10

该项主要是为了适应您的网络环境而开放出来的一种交换机缓存调度功能默认为无盘模式。它即是我们交换机几大特色之一。通过它您可以根据实际网络环境选择适合您的工作模式，以达到加速的目的。

网刻：即网络克隆，是用 TFTP 协议，通过 ghost 服务器将一个系统步署到其它客户机它主要应用于网吧及企业，电脑配置统一并且需要统一管理的环境。

无盘：即无硬盘。是当下比较流行的一种网络环境，整个网络由一台服务器及若干没有硬盘的工作站所构成。它的优点在于节约成本、抗病毒能力强等优点，广泛应用于网吧。

提示：

- 以上两种网络应用模式高度依赖于您网络的硬件平台比如网卡、网线。
- 只要网络环境不是无盘系统，请使用网刻模式。

4.3.6. 端口描述

图片 4-21

端口描述是使用一个字符串描述一个端口，以便网络管理员分清楚各个端口的用途。

端口： 对应交换机的物理端口。
描述信息：此处填写描述文字。描述信息最多可输入31个字符。

4.3.7. 端口风暴抑制

图片 4-22

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。广播风暴控制是允许交换机对网络上出现的广播帧进行过滤。当交换机发现广播帧超出一定的范围时，会自动丢弃广播帧，以防止广播风暴的发生。
交换机可以对三种常见的广播帧（广播包、组播包、单播包）进行过滤。

注意：
若端口已启用入口带宽限制，则不能启用广播风暴抑制。

4.4. 冗余与备份

4.4.1. 链路聚合

链路聚合是将交换机的多个物理端口聚合在一起形成一个逻辑上的聚合组，使得同一聚合组

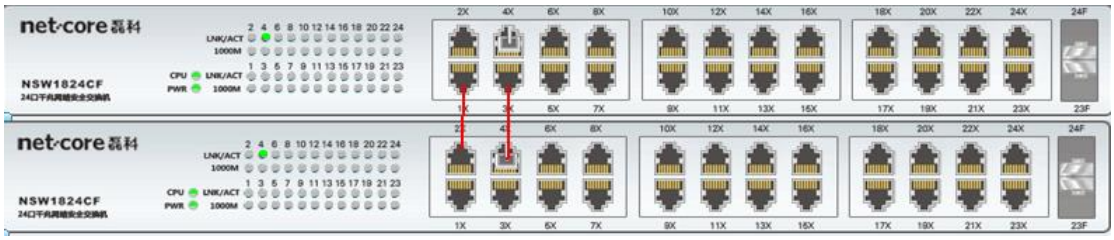
内的多条物理链路可看成一条逻辑链路。它能增加带宽和提供链路备份。链路聚合一般用来连接一个或多个带宽需求大的设备，例如连接骨干网络的服务器群或其它设备。

图片 4-230

从图片 4-上方的聚合组下拉菜单选择一个新端口，然后从左边的端口列表选择 n 个（2＜＝n＜＝8）端口，点击增加即可。选择右边聚合组端口列表相应端口号扣再点击删除按钮则完成删除操作。

聚合组总共有 8 个，从 Po1 到 Po8，而一个聚合组可以加入的最多端口数为 8 个

例如：如果我们在 NSW1824CF 聚合两个端口。那么会得到一条双向 4000M 带宽的逻辑链路。 如图片 4-所示。



图片 4-24

请按以下步骤配置：

第一步：在交换机 1 上“链路聚合”页面中的聚合组选择 Po1。

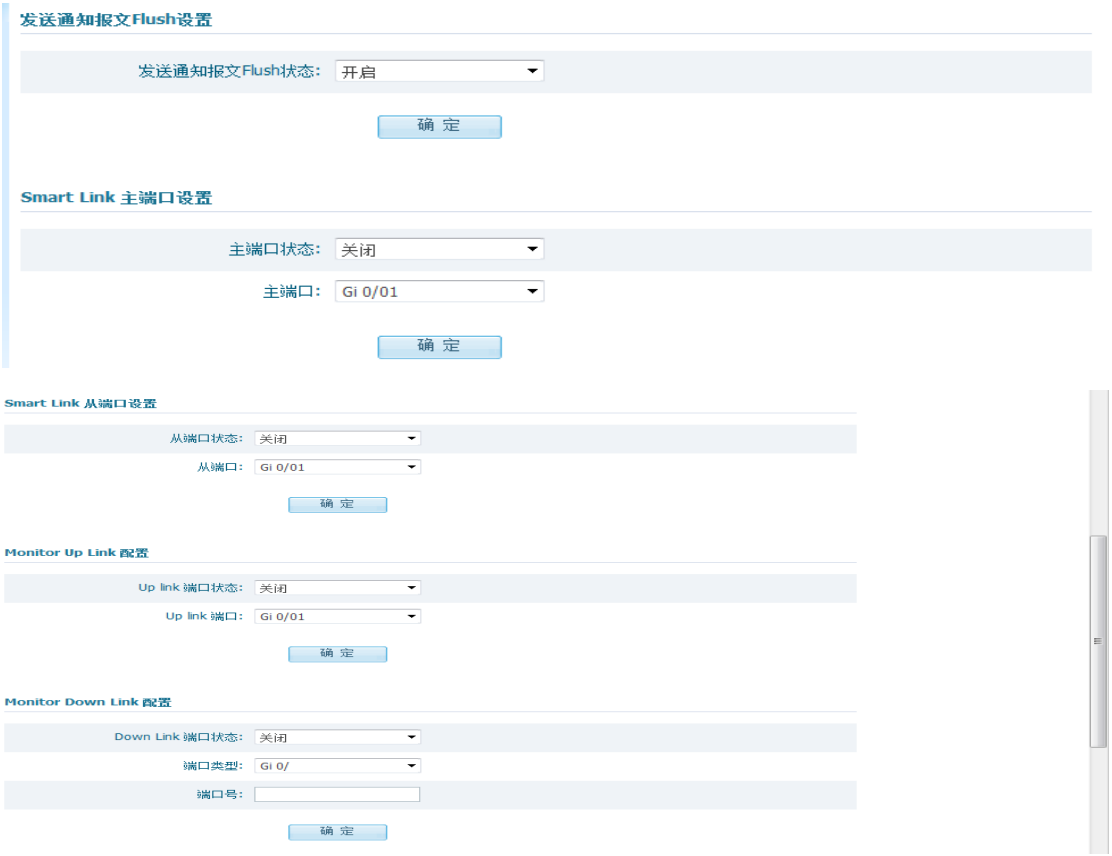
第二步：在交换机 1 的链路聚合端口列表中，选择 port1、port 3 ，单击增加按钮，将 port 1、port 3 加入到聚合组 Po1 中。

第三步：在交换机 2 上重复第二步，将 port 2、port 4 加入聚合组 Po1。

提示：

- 在相关端口加入了聚合组以后，原端口号消失，后续相关操作将基于聚合组号。
- 端口加入聚合前，需要保证该端口与聚合口下没有主机条目。
- 如果删除聚合组，绑定在该聚合口下的主机安全保护条目也将被删除。
- 该机型支持 8 组聚合组，每组最多 8 个端口。
- 链路聚合仅用于双工以太网链路。
- 聚合组中的所有链路，必须以同一速率工作。
- 不能把聚合端口用于普通连接。

4.4.2. Smart/Monitor Link 聚合

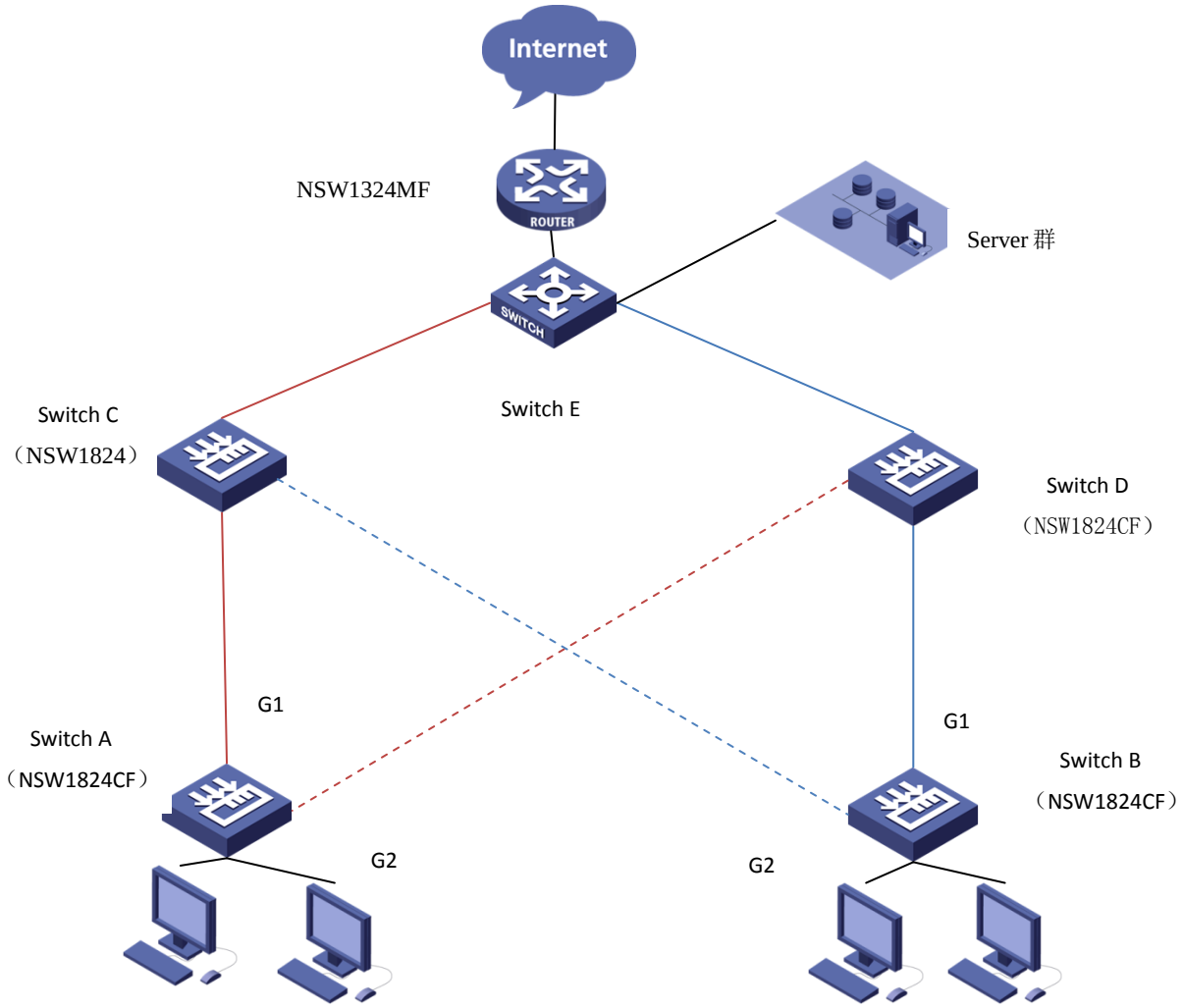


图片 4-25

Smart Link 是一种为双上行组网提供高效可靠的链路备份、负载分担和快速收敛性能的解决方案。Monitor Link 用于监控上行链路，以达到让下行链路同步上行链路状态的目的，从而触发 Smart Link 的主备链路切换，使 Smart Link 的备份作用更加完善。

4.4.2.1. smartlink 原理和配置举例

拓扑图如下，要实现图中的拓扑结构，实线为实际链路，虚线为备份链路，就可以用到 smart link 功能来设置。设置 switch A 的 G1 口为主端口 master，设置 switch A 的 G2 端口为从端口 slave；设置 switch B 的 G1 口为主端口 master，设置 switch B 的 G2 端口为从端口 slave。当 switch A 或 B 的 G1 端口出现故障时，数据会根据设置走 slave 端口的备份链路。从而达到链路备份的目的。



图片 4-26

Smart link 配置界面

如图：设置 switch A 的 G1 口为主端口 master，设置 switch A 的 G2 端口为从端口 slave，如图所示：

图片 4-27

查看设置状态为：

图片 4-28

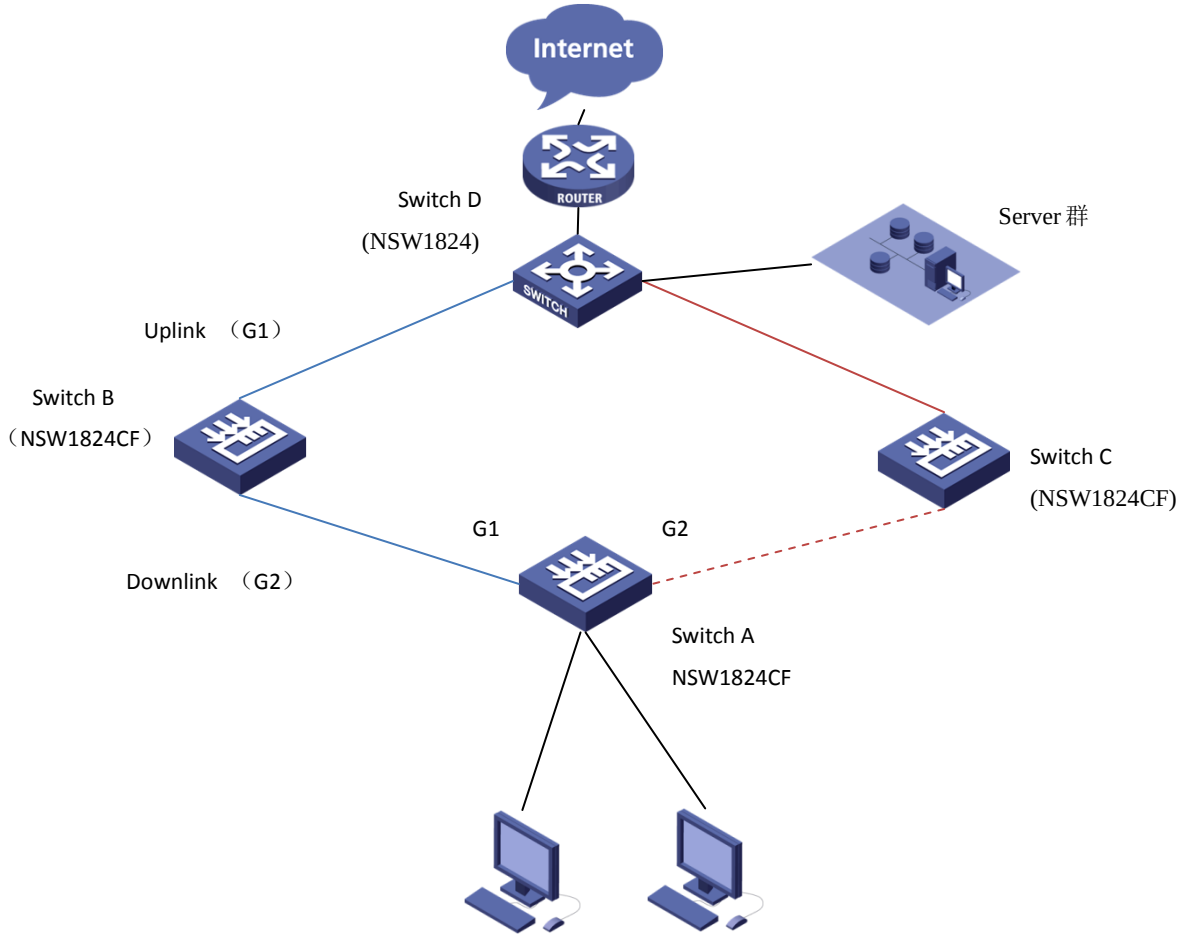
G1 口状态 active 表示正常转发，G2 口状态为 standby 为备份状态，当 G1 口链路出现故障 G2 口才进入转发状态。Smart 主从端口都可以是聚合口。

发送 flush 报文的功能是当拓扑图结构发生变化时，交换机发出 flush 报文，其他交换机收到 flush 后清空当前的动态 mac 表，达到快速收敛的效果。建议开启。

4.4.2.2. monitor link 原理和配置举例

Monitor Link 组由一个上行端口和一个或多个下行端口组成。当其上行端口所在链路发生故障时，Monitor Link 强制关闭组中所有下行端口；当上行端口所在链路恢复正常时则重新开启组内的所有下行端口。可以用来配合 smart link 功能使用。如图连接拓扑图，设置 switch

B 的 G1 口为 uplink 口，G2 为 downlink 口。Switch A 打开 smart link 功能 G1 口设置为 master 端口，G2 口设置为 slave 端口。如果没有 monitor link，当 switch B 的 G1 端口链路出现故障 down 掉了以后，switch A 并不能检测出自身 G1 端口到 internet 的链路不通，smart link 不会做出转换到备份链路的判断。当 switch B 设置了 monitor link 之后，当 switch B 的 G1 端口出现链路故障 down 时，由于 G1 是 monitor link 的 uplink 端口，所以 monitor link 的 downlink 端口即 G2 端口也会 down 掉，使得 switch A 检测出来它的 G1 链路出现故障，其 smart link 功能将调整备份链路，数据走图中红色链路。相应的 switch C 也应该开启 monitor link 功能。



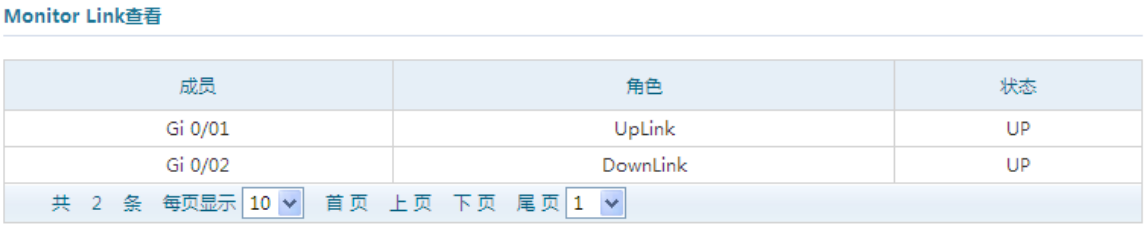
图片 4-29

Monitor link 的配置界面

如图：配置 G1 为 uplink 端口 G2 为 downlink 端口。

图片 4-30

查看 monitor link 端口状态：



图片 4-31

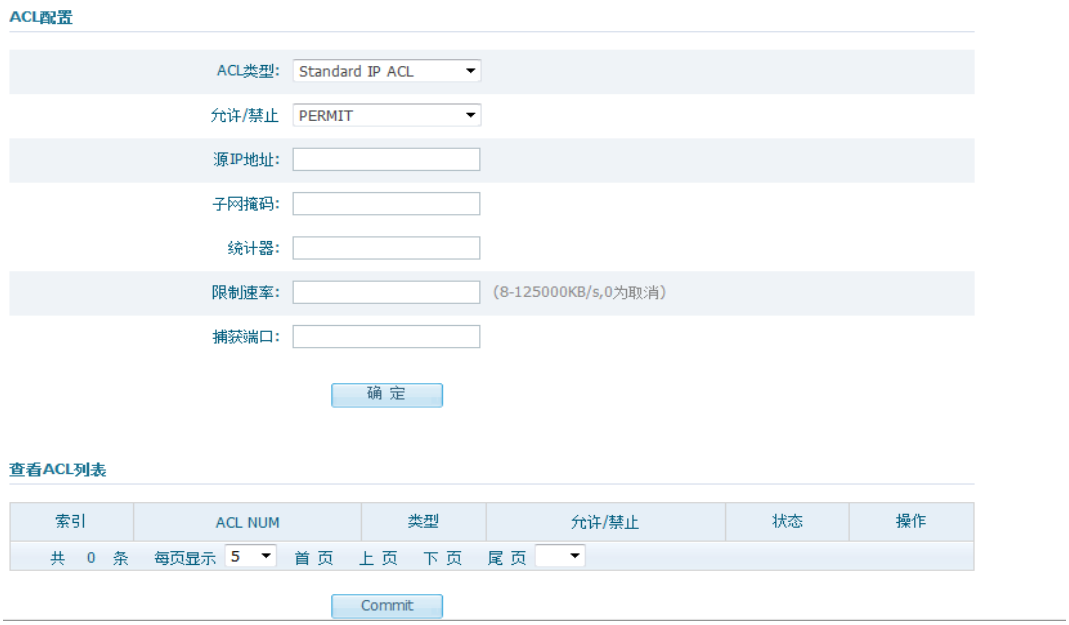
提示：

Smart Link 可以单独使用，Monitor Link 是配合 Smart Link 使用的。这些配置，只有 Monitor link 的 down-link 可以配置多个端口，其他的都只能配置 1 个端口。

4.5. 安全

通过该项可以对交换机进行安全方面的设置，以此来保障您网络安全。主要包括：ACL 设置、VLAN、MAC 地址绑定、MAC 地址过滤、MAC 地址学习、MAC 地址老化等功能。下面将详细说明。

4.5.1. ACL 设置



图片 4-32

访问控制列表可用来授权、拒绝、限制访问设备的某些特性或应用。

4.5.2. 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。

4.5.2.1. 802.1Q VLAN

802.1Q协议，即Virtual Bridged Local Area Networks协议，主要规定了VLAN的实现，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802.1Q VLAN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 802.1Q VLAN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）。PVID表示缺省端口的VLAN编号，指出从外部接收的数据帧被交换机分配到哪个VLAN去，是端口的属性。VID表示端口所处的VLAN编号，指出一个端口从交换机内部可以接受哪个VLAN的数据，是VLAN属性。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。另外，用户也可以定义某个端口同时属于多个VLAN（即VID），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。

4.5.2.2. VLAN 的相关术语

- Tagging：

将 802.1Q VLAN 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。

- Untagging：

将 802.1Q VLAN 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。

- Access 链路：

即 Untagging，是将 802.1Q VLAN 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。

- 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 802.1Q VLAN 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。

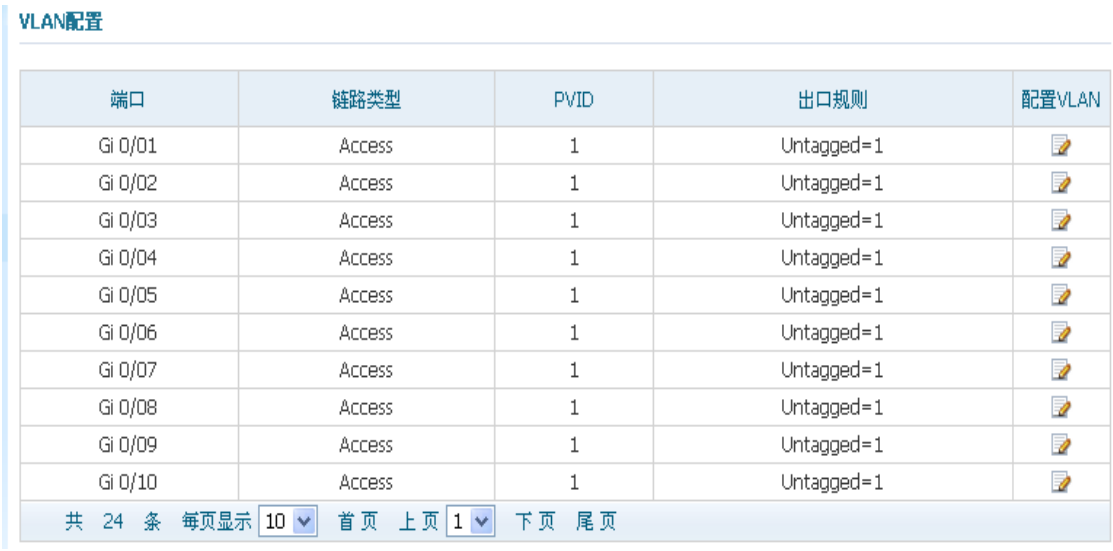
- Hybrid 链路：

Hybrid 端口和 Trunk 端口在接收数据时，处理方法是一样的，唯一不同之处在于发送数据时： Hybrid 端口可以允许多个 VLAN 的报文发送时不打标签，而 Trunk 端口只允许缺省 VLAN 的报文发送时不打标签

- PVID：是端口所属的 VID 号。

4.5.2.3. VLAN 的设置方法

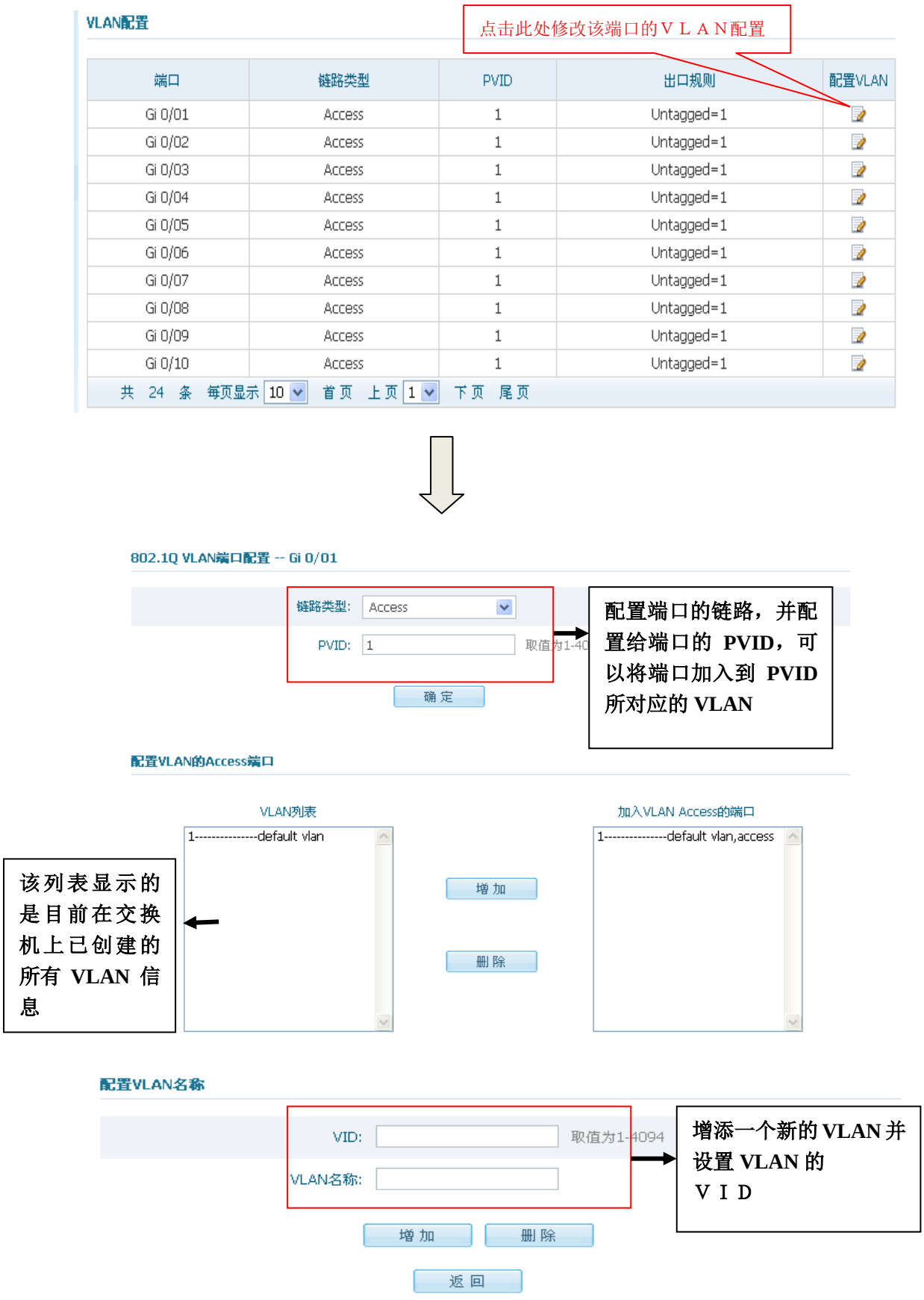
第一步、点击“安全”下的“VLAN”，您可以看见所有端口的VLAN信息显示。



图片 4-33

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，首先点击某一个端口的“配置 VLAN”选项可以修改此端口的 VLAN 配置。例如点击端口 1，出现 VLAN 端口配置信息，如下图所示

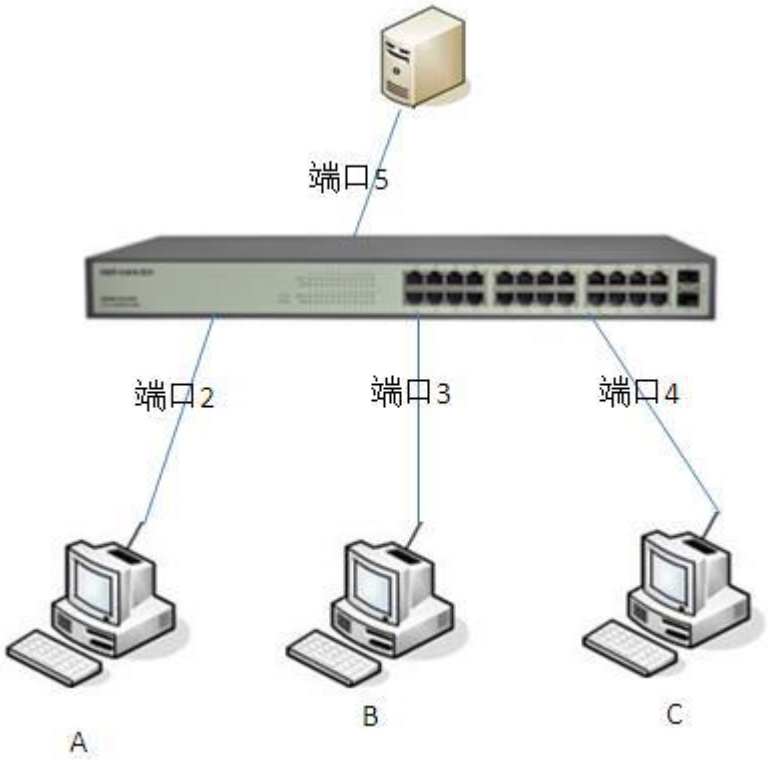
第二步、点击您所需要设定的端口，进入设置界面。


VLAN配置
点击此处修改该端口的ＶＬＡＮ配置
端口
链路类型
PVID
出口规则
配置VLAN
Gi 0/01 Access 1 Untagged=1
Gi 0/02 Access 1 Untagged=1
Gi 0/03 Access 1 Untagged=1
Gi 0/04 Access 1 Untagged=1
Gi 0/05 Access 1 Untagged=1
Gi 0/06 Access 1 Untagged=1
Gi 0/07 Access 1 Untagged=1
Gi 0/08 Access 1 Untagged=1
Gi 0/09 Access 1 Untagged=1
Gi 0/10 Access 1 Untagged=1
共 24 条 每页显示 10 首页 上页 1 下页 尾页
802.1Q VLAN端口配置 -- Gi 0/01
链路类型: Access
PVID: 1
取值为1-40
确 定
配置端口的链路，并配置给端口的 PVID，可以将端口加入到 PVID 所对应的 VLAN
配置VLAN的Access端口
VLAN列表
1----------default vlan
该列表显示的是目前在交换机上已创建的所有 VLAN 信息
增 加
删 除
加入VLAN Access的端口
1----------default vlan,access
配置VLAN名称
VID:
取值为1-4094
VLAN名称:
增 加
删 除
返 回
增添一个新的 VLAN 并设置 VLAN 的 ＶＩＤ

图片 4-34

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。



图片 4-35

上图所示主机，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

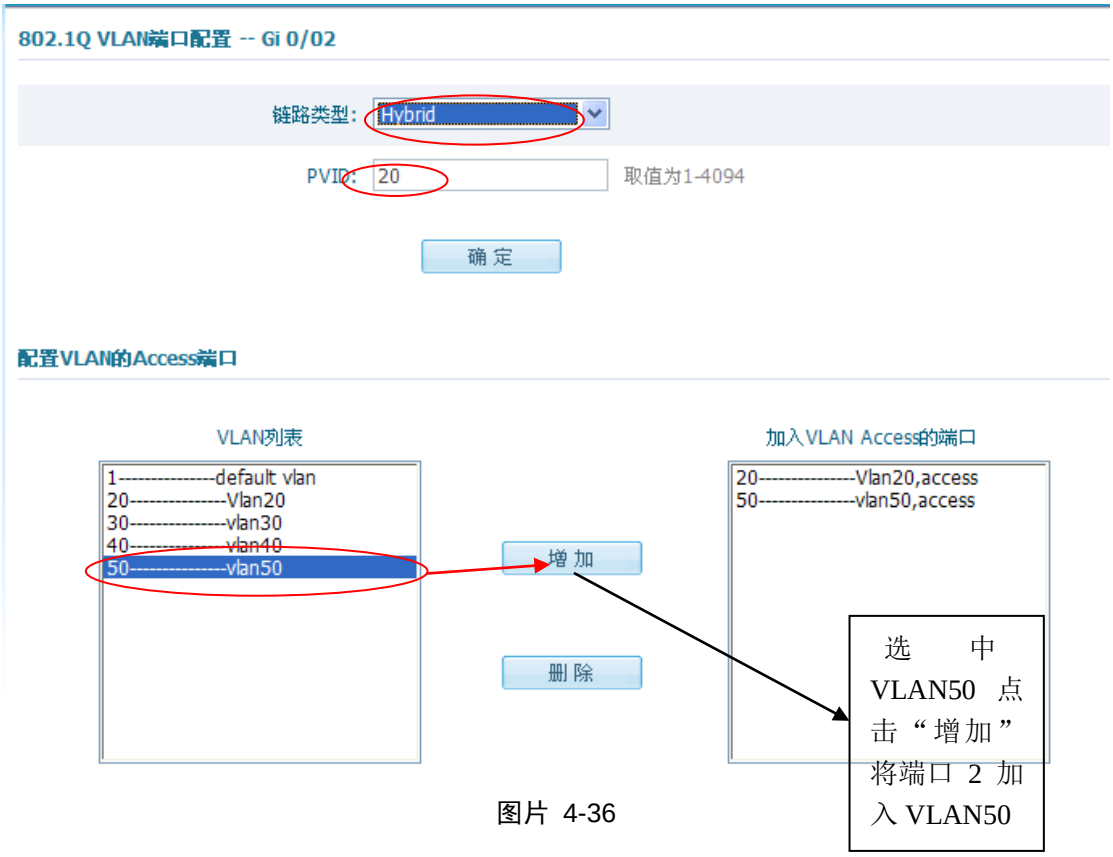
VLAN	成员端口
VLAN20	2、5
VLAN30	3、5
VLAN40	4、5
VLAN50	2、3、4、5

端口	PVID
5	50
2	20
3	30
4	40

1、 依次创建 VLAN20、VLAN30、VLAN40、VLAN50

2、端口 2 的配置方法：

将 port2 的 PVID 设置为 20，将链路类型设置为：Hybrid，将端口 2 加入到 VLAN50 中



图片 4-36

3、端口 3 的配置方法：

将 Port 3 的 PVID 值设置为 30 ， 链路类型为：Hybrid，将端口 3 加入到 VLAN50 中

图片 4-37

4、端口 4 的配置方法：

将 Port 4 的 PVID 值设置为 4，链路类型为：Hybrid，将端口 4 加入到 VLAN50 中

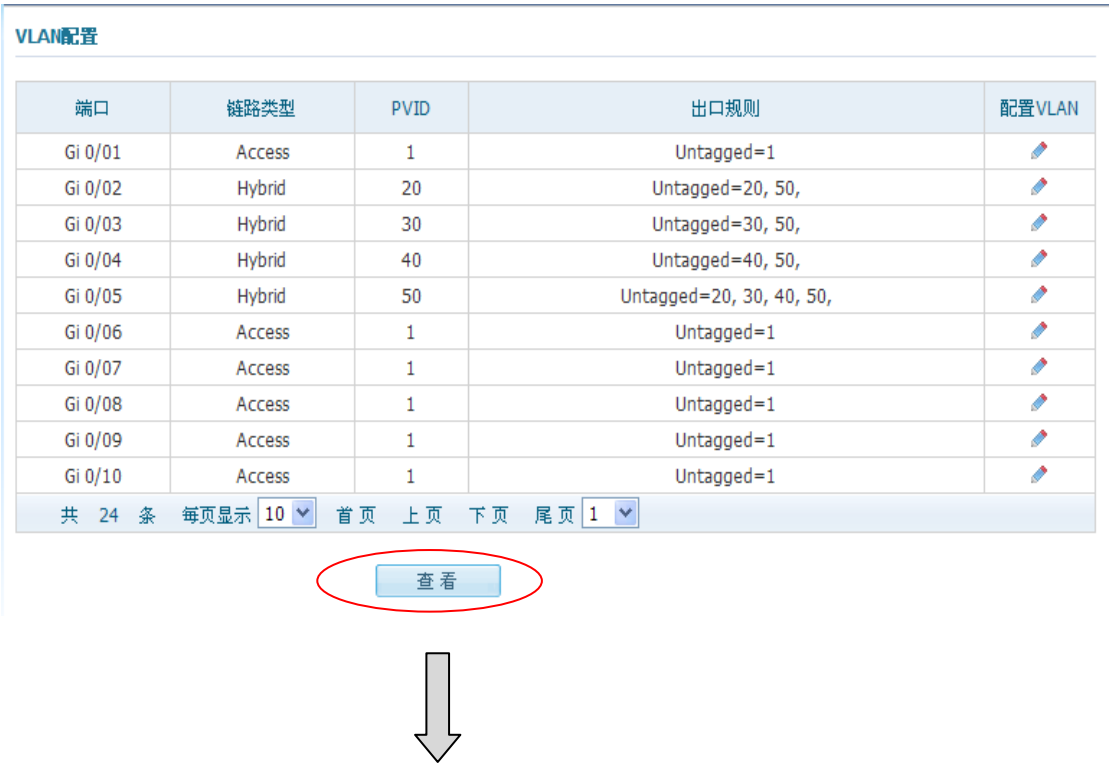
图片 4-38

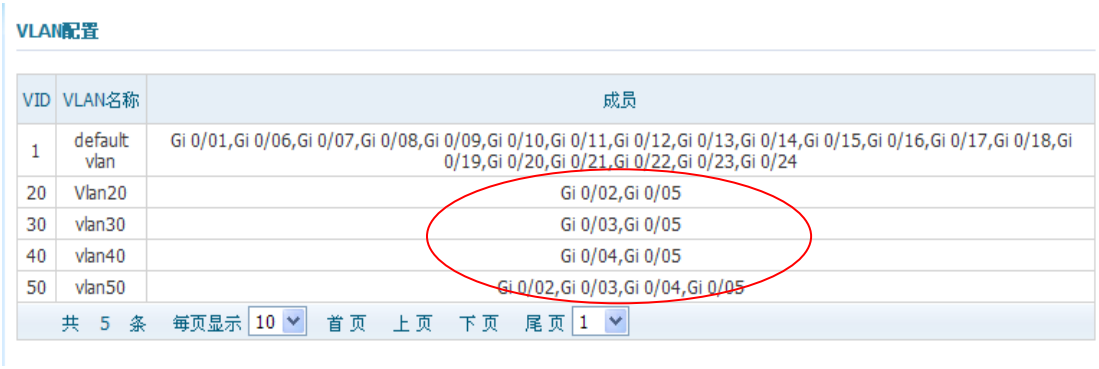
5、端口 5 的配置方法：

将 Port 5 的 PVID 值设置为 50，链路类型为：Hybrid，将端口 5 加入到 VLAN20、VLAN30、VLAN40 中。

图片 4-39

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





图片 4-39

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。

- 首先创建 VLAN2 和 VLAN3

图片 4-43

创建VLAN3类似。

- 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 4-44

➢ 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 4-45

➢ 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 4-46

- 配置完成后可以去查看所有 VLAN 的配置信息

VLAN配置

端口	链路类型	PVID	出口规则	配置VLAN
Gi 0/01	Access	2	Untagged=2	
Gi 0/02	Trunk	2	Tag=3,Untagged=2,	
Gi 0/03	Access	3	Untagged=3	
Gi 0/04	Hybrid	1	Untagged=1,	
Gi 0/05	Hybrid	1	Untagged=1,	

图片 4-47

- 再查看 VLAN 的成员列表

VLAN配置

VID	VLAN名称	成员
1	default vlan	Gi 0/04,Gi 0/05,Gi 0/06,Gi 0/07,Gi 0/08,Gi 0/09,Gi 0/10,Gi 0/11,Gi 0/12,Gi 0/13,Gi 0/14,Gi 0/15,Gi 0/16,Gi 0/17,Gi 0/18,Gi 0/19,Gi 0/20,Gi 0/21,Gi 0/22,Gi 0/23,Gi 0/24
2	Vlan2	Gi 0/01,Gi 0/02
3	Vlan3	Gi 0/02,Gi 0/03

共 3 条 每页显示 10 首页 上页 1 下页 尾页

图片 4-48

4.5.3. MAC 地址绑定

4.5.3.1. MAC 地址绑定原理

MAC 地址绑定是 NSW1824CF 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就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。将端口号和 MAC 地址绑定后，可以比较有效的防止 ARP 欺骗。

4.5.3.2. MAC 地址的绑定配置

例如：将一台 MAC 地址为 D4-BE-D9-D1-6C-0A 的设备限制在 NSW1824CF 交换机的 1 号端口上使用，VID 值为 2，具体操作如下：

在“MAC 地址”框中输入 D4-BE-D9-D1-6C-0A，然后在“端口号”框选中“Gi0/01”，输入 VID 值 2，点击“增加”

图片 4-49

提示：

- 绑定后的设备只能在绑定端口上通信，但该端口仍然允许其它设备与此交换机通信。
- 同一个端口下可以绑定多个设备 MAC。
- 同一个设备不能同时被绑定与过滤。

- 绑定后的设备将不受 MAC 地址动态学习影响。

4.5.4. MAC 地址过滤

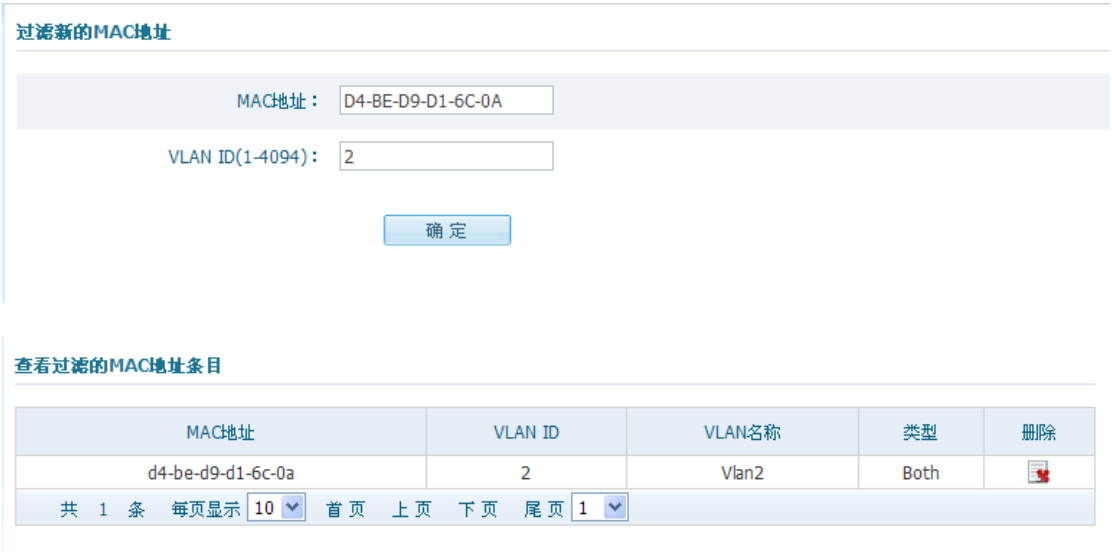
4.5.4.1. MAC 地址过滤原理

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。

4.5.4.2. MAC 地址过滤配置

把 NSW1824CF 交换机的属于 VLAN2 的一台 PC 的 MAC 地址（PC 网卡的 MAC 地址为 D4-BE-D9-D1-6C-0A）进行过滤，具体操作如下：

在“MAC 地址”框中输入 D4-BE-D9-D1-6C-0A，点击“增加”，如下图所示：



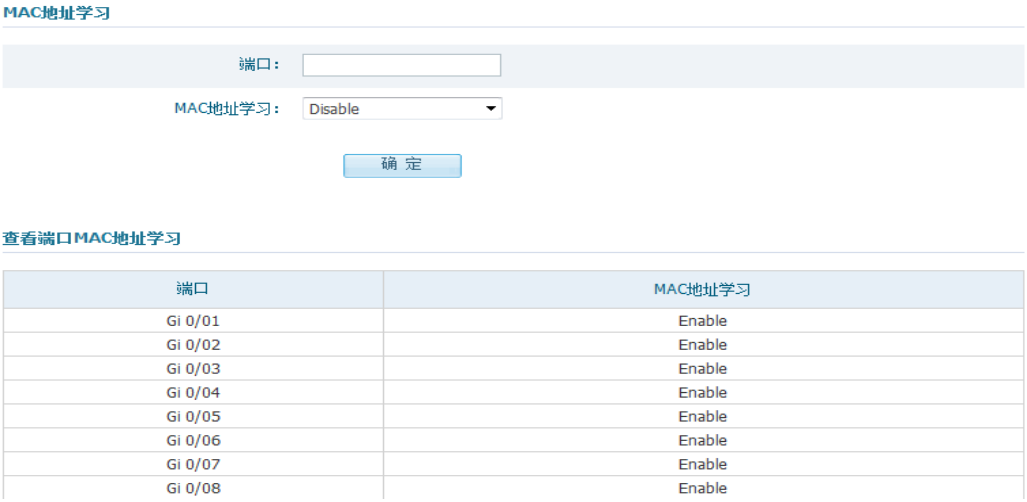
图片 4-50

地址里面填写要过滤的 MAC 地址，选择过滤类型及隶属的 VLAN ID 它即会出现在当前过滤的 MAC 地址表中。

4.5.5. MAC 地址学习

4.5.5.1. MAC 地址学习原理

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。如果某一个端口的MAC地址学习状态为Disable，除了已静态绑定的设备以外的其它设备都将无法与交换机通信。

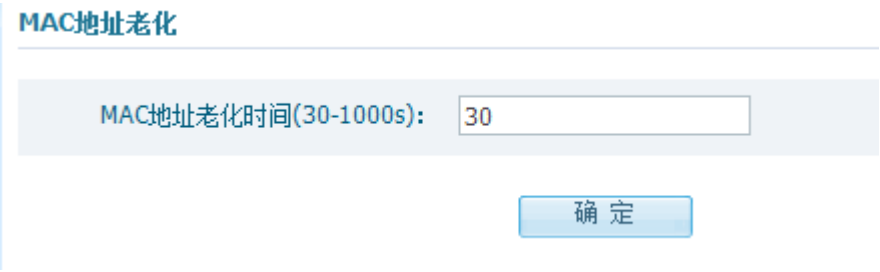


图片 4-51

- 端口：每一个端口对应一个 MAC 地址学习状态
- MAC 地址学习：输入端口号以及 MAC 地址学习状态 enable 或 disable

4.5.6. MAC 地址老化

交换机内部维护了着一张动态 MAC 地址表。这张表是数据通信的关键。动态MAC 地址表有两项内容：MAC 地址及其对应的端口号。动态地址表是动态更新的，表里的每一个记录都有寿命，其寿命的长短是受老化时间控制。如果该记录在寿命内没有被重新学习，那么它将会被删除，这个过程就叫做“老化”。这个寿命的长短就是“老化时间”，单位为秒。



图片 4-52

- MAC 地址老化时间：输入 MAC 地址老化时间，范围为 30-1000s。默认为 30 秒。

提示：

- 老化时间过长会长期占用有限的 MAC 表空间，造成转发混乱。老化时间过短造成 MAC 表刷新过快，影响转发速度。因此慎用些功能。一般采用默认值。
- 老化时间无法约束已存在的静态的 MAC 地址。

4.6. QoS

4.6.1. QoS 配置信息

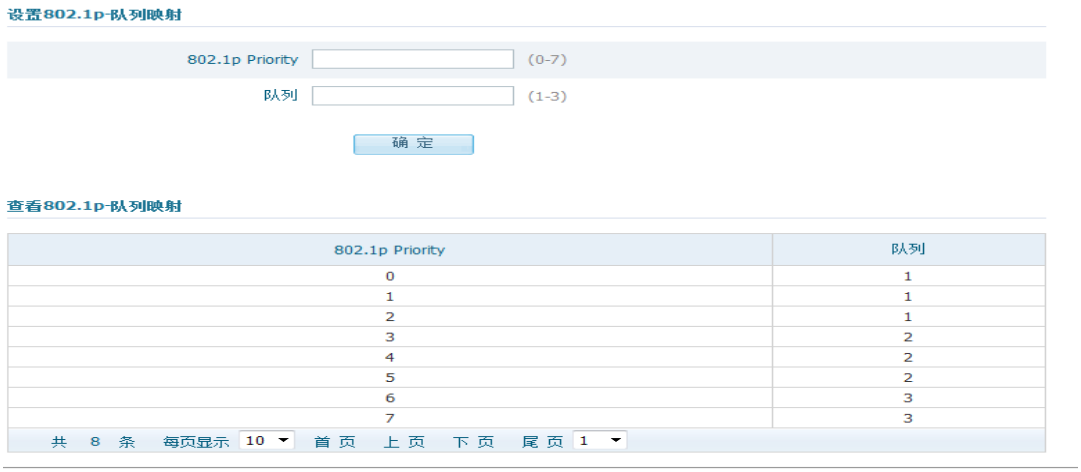
QoS（Quality of Service）即服务质量，在 Internet 中用来表征网络服务的好坏。通常所说的 QoS，是针对各种网络应用的不同需求，为其提供不同的服务质量，如提供专用带宽，减少报文丢失率，降低报文传送时延及时延抖动等。即在带宽不充裕的情况下，对各种服务流量占用带宽的矛盾做一个平衡。QoS 配置信息给出了信任模式，调度策略，队列配额的详细参数。

图片 4-53

4.6.2. 802.1P-队列映射

802.1P 优先级就是根据Pri 的域值来决定数据帧的优先级。每一个802.1Q Tag 中都有一个Pri 域，该域由三个bit 为组成，取值范围是0~7。通过交换机的配置页面可配置不同的Pri域对应不同的优先级，交换机发送数据帧时，会根据数据帧的Tag 决定发送的优先级。对于Un tagged帧，交换机则按照该入口端口的默认优先级对数据帧进行QoS 处理。

当启用 802.1P 优先级时，根据数据包是否带有802.1Q Tag 确定使用哪种优先级模式。对于带有Tag的数据包，应用802.1P 优先级；否则应用Port 优先级。当启用DSCP 优先级的时候，如果数据包是IP 包，则应用DSCP 优先级；对于非IP 包，交换机则根据是否启用802.1P 优先级以及数据帧是否带有Tag 来决定采用哪种优先级模式。



图片 4-54

4.6.3. 端口默认优先级

端口优先级有八个优先等级，分别对应到出口队列的 0- 7，表示从该端口接收到的所有数据帧都被指定为设定的优先级，其中 0 对应最低优先级的队列，7 对应最高优先级的队列。

图片 4-55

4.7. 组播管理

该功能是 2+4 层管理型交换机的最重要的功能之一，它被广泛应用于网吧或是大中型企业需要网络克隆的环境。它不仅操作方便而且更能成倍的节约网克时间。其工作原理我们这里就不再赘述。下面我们就以如何在实际当中使用做详细的说明，该项主要包括：IGMP Snooping 和组播路由端口两个子项。

4.7.1. 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 4-56

- IGMP Snooping 状态：一般采用默认状态，默认状态为 Enable。

4.7.2. 组播路由端口

图片 4-57

组播路由端口：交换机上连接组播路由器的端口。

VID：即组播成员所在的 VID 号。比如组播成员在 VID1 就填写 VID1。

组成员老化时间：交换机为该端口启动一个定时器，其超时时间就是组成员老化时间。

动态路由老化时间：交换机为每个动态路由连接口启动一个定时器，其超时时间就是动态路由老化时间。

例如：拓扑结构为网刻服务器接中心交换机 NSW1824，接入层为两台 NSW1824CF 时，要求 1824CF1 与 1824CF2 下的ＰＣ机全部进行网刻，1824CF 下的ＰＣ机照常应用。并且两者互不影响。网刻服务器接在 NSW1824 的 1 号端口，1824CF1 的 1 号端口与 1824 的 2 号端口相连，1824CF2 的 2 号端口与 1824 的 3 号端口相连。则按下述步骤操作。

- 进入交换机 NSW1824“组播路由端口”管理界面，在端口列表里和 VID 列表里填 1 后点击增加按钮。
- 进入交换机 NSW1824CF1“组播路由端口”管理界面，在端口列表里填 1 ,VID 号填 1 后点击增加按钮。
- 进入交换机 NSW1824CF2“组播路由端口”管理界面，在端口列表里填 2 ,VID 号填 1 后点击增加按钮。
- 在服务器端运行网刻软件并重启ＰＣ机进行网刻。
- 打开 NSW1824CF 组播管理界面，这里会显示正在进行组播的组信息。

至次所有设置操作均已完毕。

注意：

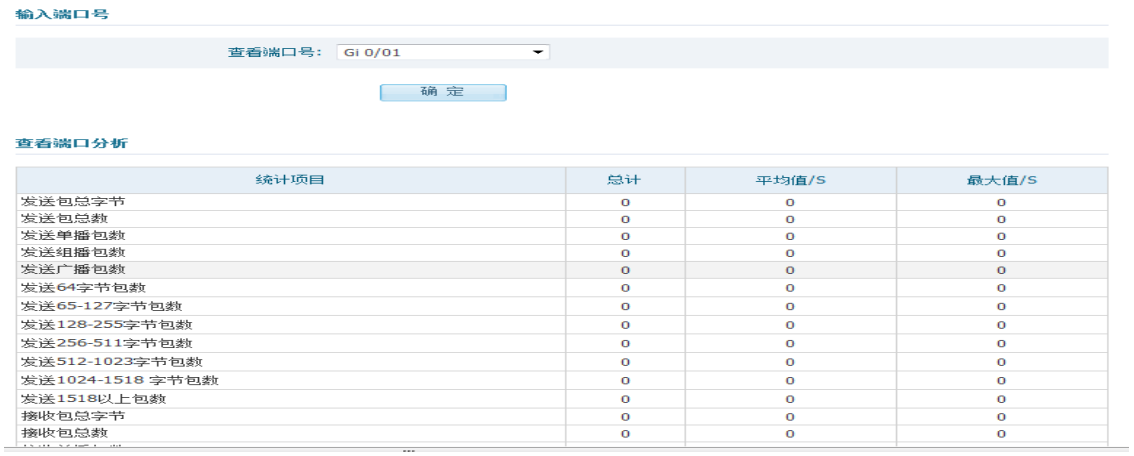
- 网刻速度高度依赖于你网卡及网线的质量。
- 网刻时不同速率的网卡会互相影响，所以请使用同一种速率的网卡进行网刻。

4.8. 网络分析

网络分析包括：端口分析、端口镜像、ARP 攻击日志。下面详细说明

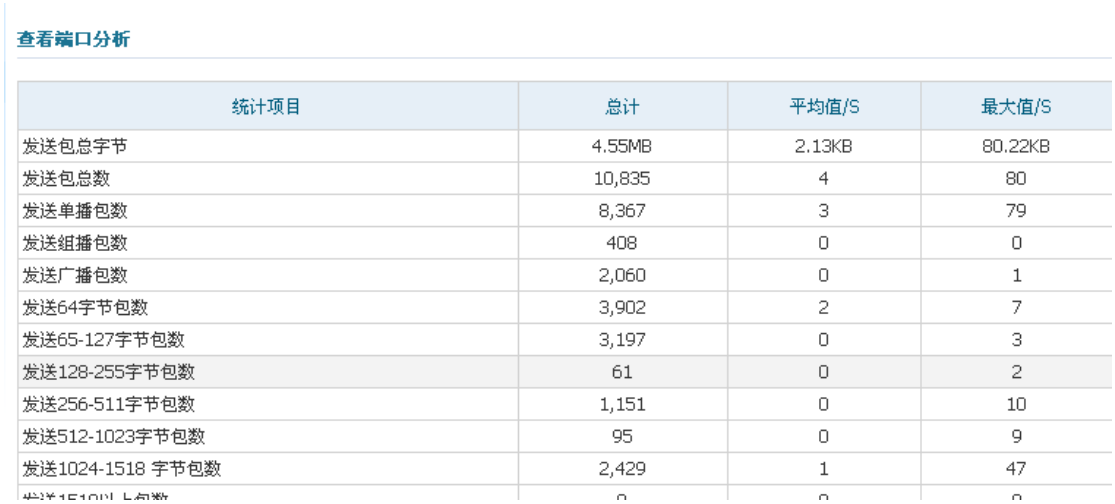
4.8.1. 端口分析

此功能显示了端口当前的数据收发状态其中包括发包总数、收包总数、接收/发送字节数等信息。它可以为您进行网络维护提供一个参考。



图片 4-58

在查看端口号里面选择要查看的端口号，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 4-59

4.8.2. 流量统计

流量统计针对每一个端口，统计它收发多少数据字节、多少个数据帧、多少个广播帧、多少个多播帧、多少个错误帧等等。

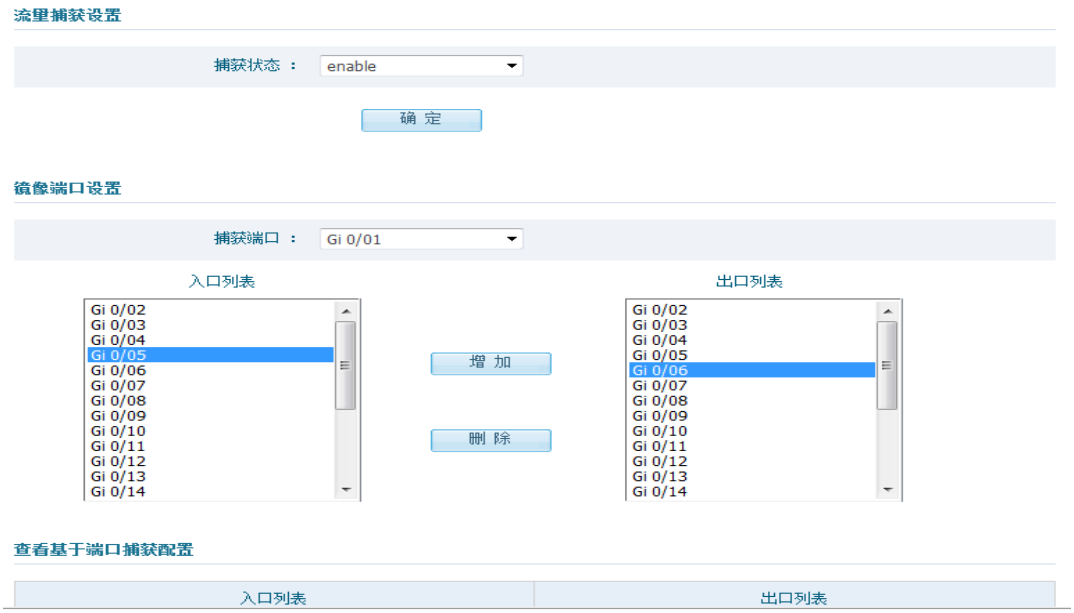
图片 4-60

4.8.3. 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：用端口 1 去捕获端口 5 到端口 6 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“入口列表”输入“5”，在“出口列表”输入“6”，点击“增加”，查看捕获器中会显示配置的条件。



图片 4-61

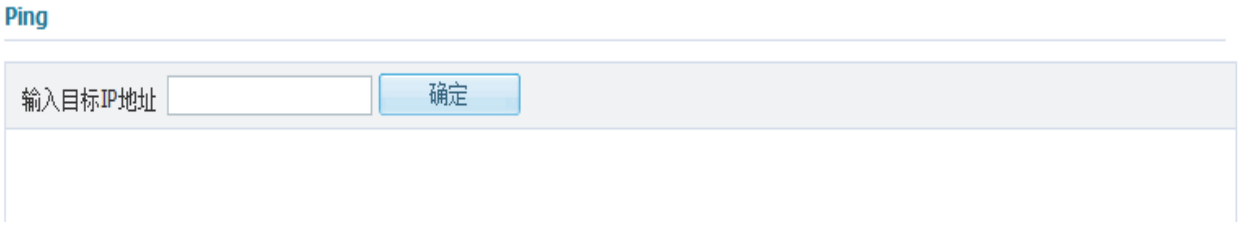
4.8.4. ARP/IP 攻击

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

图片 4-62

4.8.5. PING

此处增加了 ping IP 地址的功能。



图片 4-63

4.8.6. 日志

此处增加了日志记录设置及显示日志列表的功能。

图片 4-64

可以选择开启各种功能及系统的记录日志，默认为全部关闭。

4.9. DHCP Snooping

DHCP Snooping 技术是 DHCP 安全特性，通过建立和维护 DHCP Snooping 绑定表过滤不可信任的 DHCP 信息，这些信息是指来自不信任区域的 DHCP 信息。DHCP Snooping 绑定表包含不信任区域的用户 MAC 地址、IP 地址、租用期、VLAN-ID 接口等信息。

当交换机开启了 DHCP-Snooping 后，会对 DHCP 报文进行侦听，并可以从接收到的 DHCP Request 或 DHCP Ack 报文中提取并记录 IP 地址和 MAC 地址信息。另外，

DHCP-Snooping 允许将某个物理端口设置为信任端口或不信任端口。信任端口可以正常接收并转发 DHCP Offer 报文，而不信任端口会将接收到的 DHCP Offer 报文丢弃。这样，可以完成交换机对假冒 DHCP Server 的屏蔽作用，确保客户端从合法的 DHCP Server 获取 IP 地址

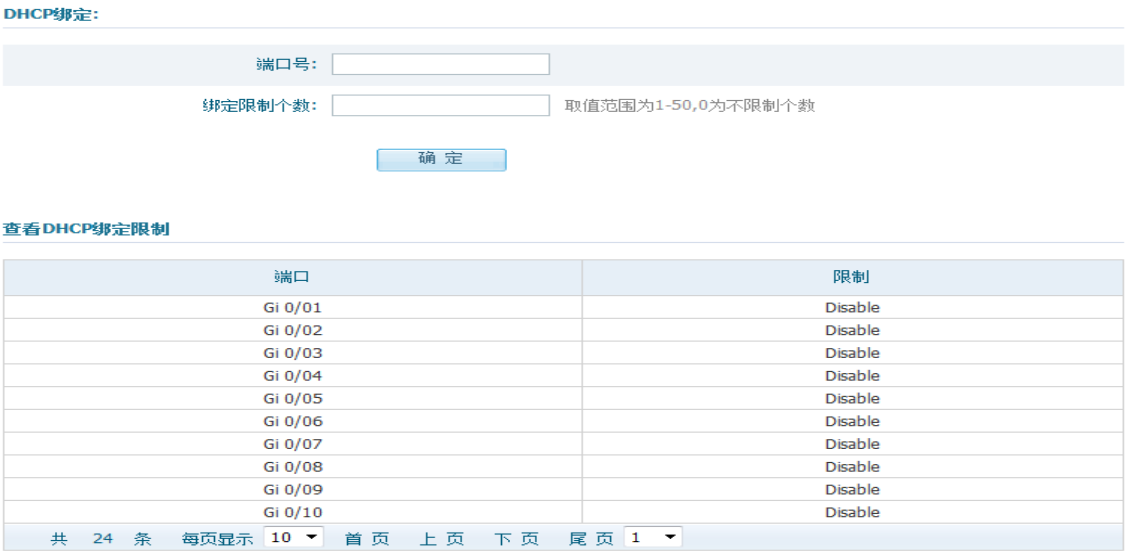
4.9.1. DHCP 设置

该选项用于开启关闭 DHCP Snooping 功能

图片 4-65

4.9.2. DHCP 绑定

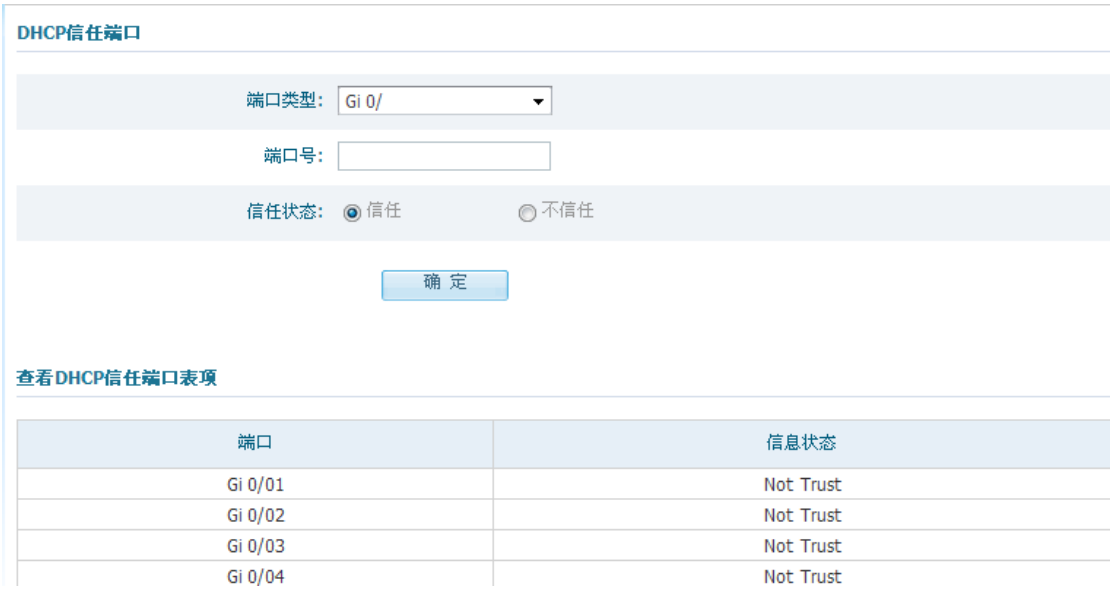
该选项用于分配每个端口可以绑定的 IP 地址个数，最多可以绑定两个 IP 号。



图片 4-66

4.9.3. DHCP 信任端口

设置每个端口为信任端口或是不信任端口，信任端口：与合法的 DHCP 服务器直接或间接连接的端口。信任端口可以正常接收并转发 DHCP Offer 报文，而不信任端口会将接收到的 DHCP Offer 报文丢弃。



图片 4-67

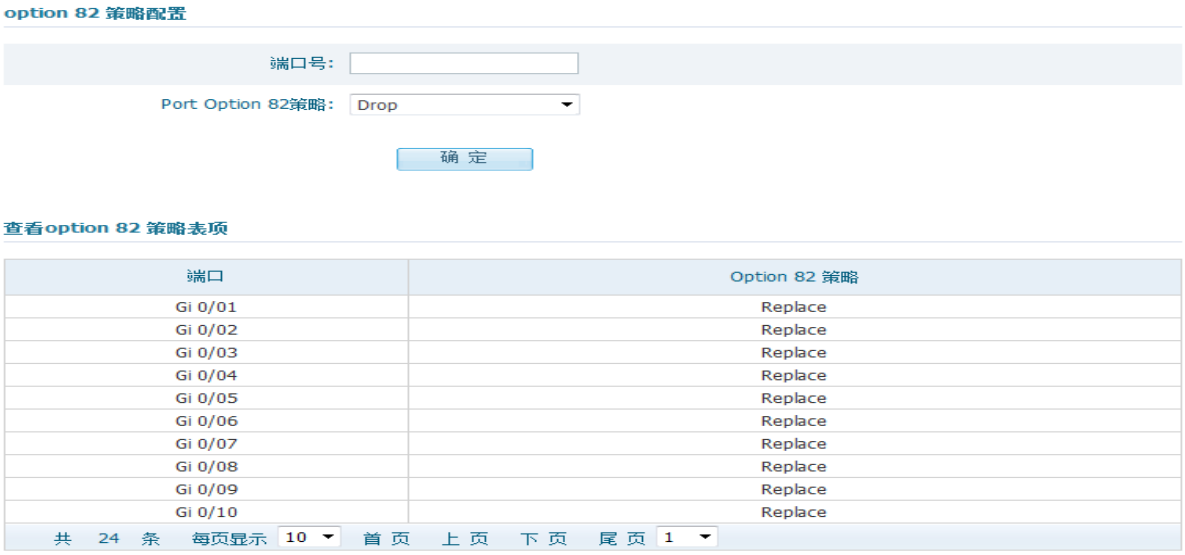
4.9.4. Option82 配置

图片 4-68

该项目用来填写端口 Option82 进行配置：

端口号:填入需要分配 IP 的主机连接交换机的实际端口
端口索引：即端口号，此处填入实际端口号
VLAN ID：填入 VLAN 号即端口所属 VLAN
Remote id:填入接入交换机的 MAC 地址，如:22-22-22-22-22-22

4.9.5. Option82 策略



图片 4-69

此处填写 option82 各个端口策略情况，含三种分别是 Drop、Keep 和 Replace。

4.9.6. ARP 设置

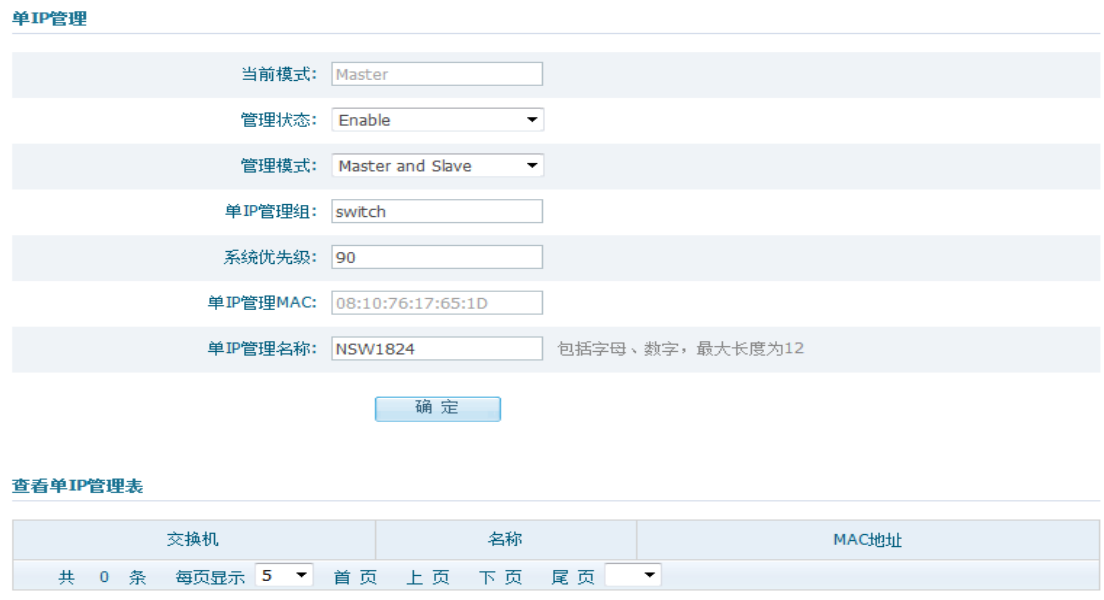
对绑定的不信任端口进行 ARP/IP Filter，建立和维护一张 dhcp-snooping 的绑定表，这张表一是通过 dhcp ack 包中的 ip 和 mac 地址生成的，二是可以手工指定。这张表是后续 DAI（dynamic arp inspect）和 IP Source Guard 基础。这两种类似的技术，是通过这张表来判定 ip 或者 mac 地址是否合法，来限制用户连接到网络的；

图片 4-70

4.10. 联动管理

主要包括：联动管理、参数分发和批量升级。下面将详细说明。

4.10.1. 联动管理



图片 4-71

该功能既我们常说的联动网管功能。通过对该页面里相关参数的设置。可以方便管理局域网中其它交换机设备。

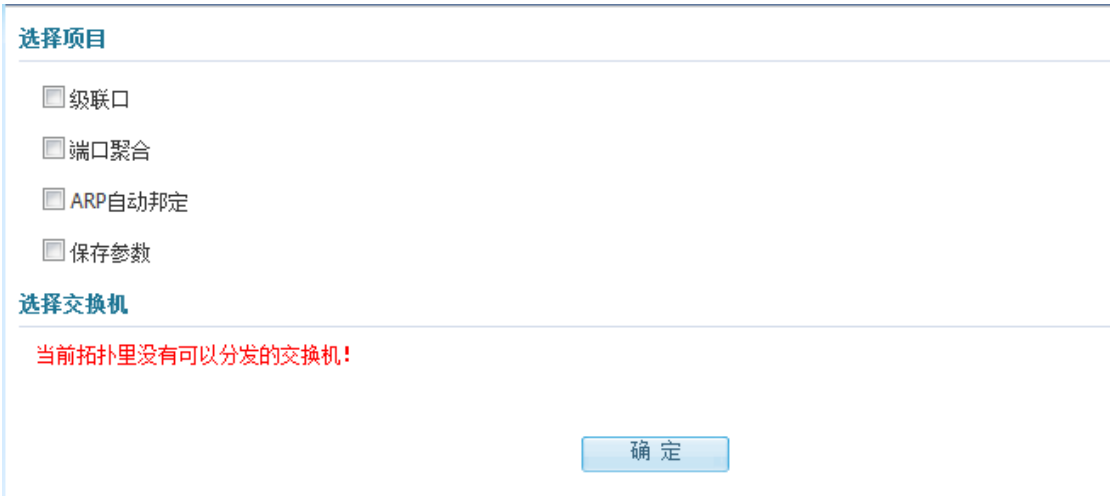
- 当前模式：显示当前登录的交换机的状态是管理者还是被管理者；默认为管理交换机。
- 管理状态：联动网管功能的开关，当为 Enable 时联动网管功能生效，当为 Disable 时联动网管功能失效；默认为 Enable。

- 管理模式：当前交换机的管理模式包括管理交换机与客户机两种状态；默认为管理交换机
- 联动管理组：用于识别当前登录的交换机属于那个分组；默认为 switch。
- 系统优先级：用于竞选管理者交换机的依据之一；不同型号略有不同，该型号默认为 100。
- 设备 MAC：用于竞选管理者交换机的依据之一；交换机不同而不同。
- 设备名称：用于标识交换机，以与其它交换机相区分。交换机不同而不同。该型号默认为 NSW1824CF 2+4 层安全交换机。

提示：

- 管理交换机的竞选规则遵循优先匹配“系统优先级”然后匹配“设备 MAC”的原则，谁最小谁就是管理者。
- 一般用户只需更改“设备名称”即可，其它参数请使用默认设置。
- 如果交换管理端口的变更，将影响访问效果。

4.10.2. 参数分发



图片 4-72

该功能用来对整个拓扑里面交换机进行参数分发，减少人工作业，有效节省人力成本。

4.10.3. 批量升级

图片 4-73

该功能用来对整个拓扑的相同型号的交换机进行升级，目前支持 NSW1324MF，NSW1824CF 以及 NSW1824 三款产品。

4.11. 网络设备维护

主要包括：主机安全保护、应用程序优先级、环路检测、单向链路检测、ARP 自动绑定、防蠕虫攻击。

4.11.1. 主机安全保护

图片 4-74

主机安全保护可以对开启可以对主机进行安全保护，默认关闭。用户可以通过保护策略——含安全策略和绑定策略，查询网络设备属性了解整网设备情况狂，还可以通过添加网络设备来对下联交换或者设备进行保护。

4.11.2. 应用程序优先级

图片 4-75

应用程序优先级用来调节数据包优先转发，能够有效保证用户带宽。现支持魔兽世界，CS，锐起无盘等程序。优先级含高优先级，普通优先级和低优先级三种。

4.11.3. 环路监测

图片 4-76

该功能可以有效的检测出下联拓扑中出现的环路情况，默认为关闭。在使用时点击“开启”，报文数跟检测时间可不做更改，其表示每 30s 发一个环路检测报文。端口环路监测设置指对特定的端口进行环路检测，有三个方式，interval 表示间隔发送环路检测报文，always 表示一直发送环路检测报文，close 表示关闭该端口的环路检测功能，你只有开启环路检测并对其中某一个端口进行环路检测，环路检测才会生效。例如当环路出现时，环路检测信息里面端口会出现如下显示，表示检测到了 10 端口有环路并阻塞了该端口，避免其影响到其他端口正常工作，配置和现象如下：

图片 4-77

注意：

本交换机只能对检测下联网络是否有环路，不能对本机进行环路检测。

4.11.4. 单向链路检测

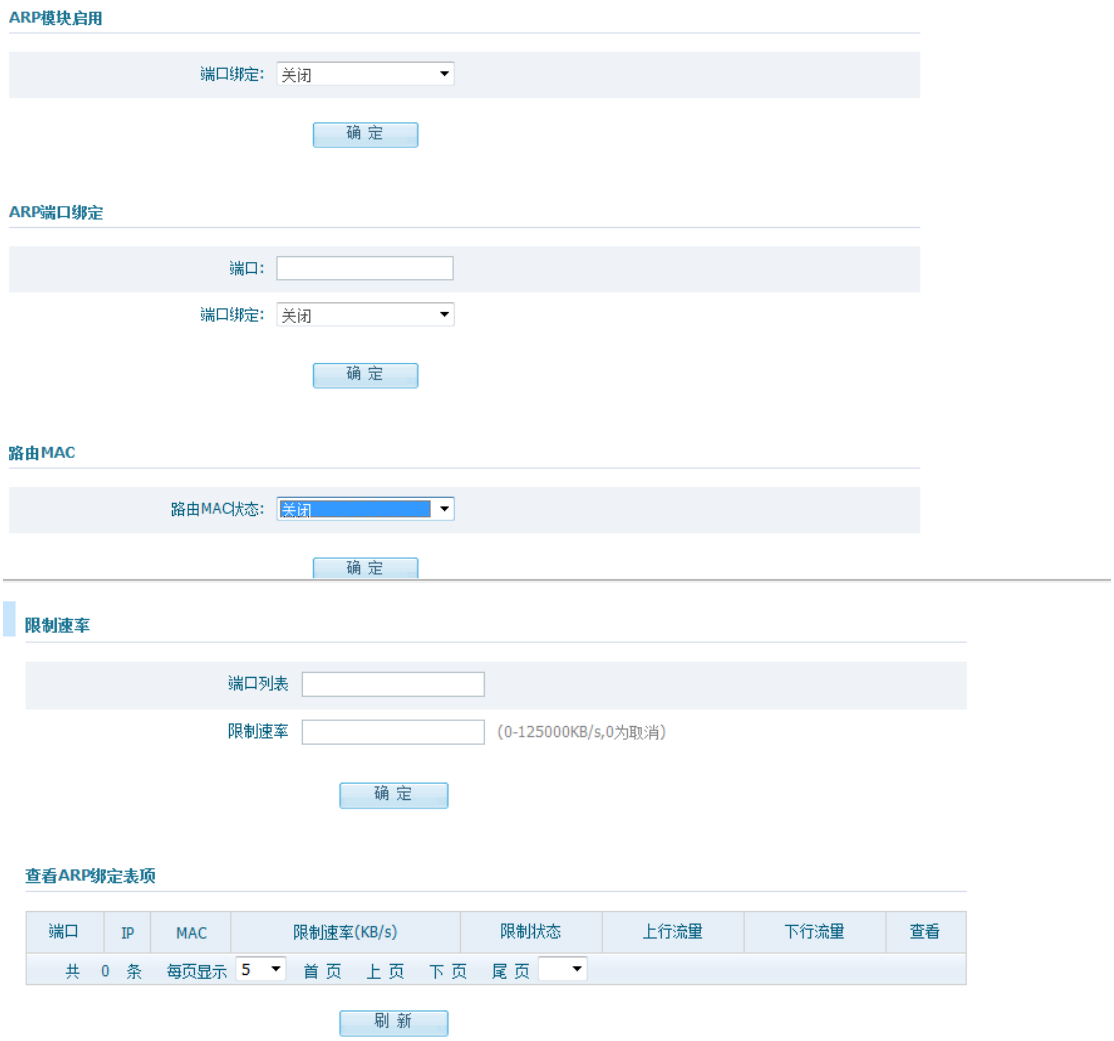
图片 4-78

该功能用来检测两个交换机互相连接的端口能否正常通信。

注意：

如果端口开启此功能的话，将不能通信，除非对方设备也是开启此功能才能正常进行协商检测。如果检测有问题，会有提示，如果正常的话，就可以正常通信。因此建议最好先开启远端设备端口的这个功能，再来开近端设备端口的这个功能。

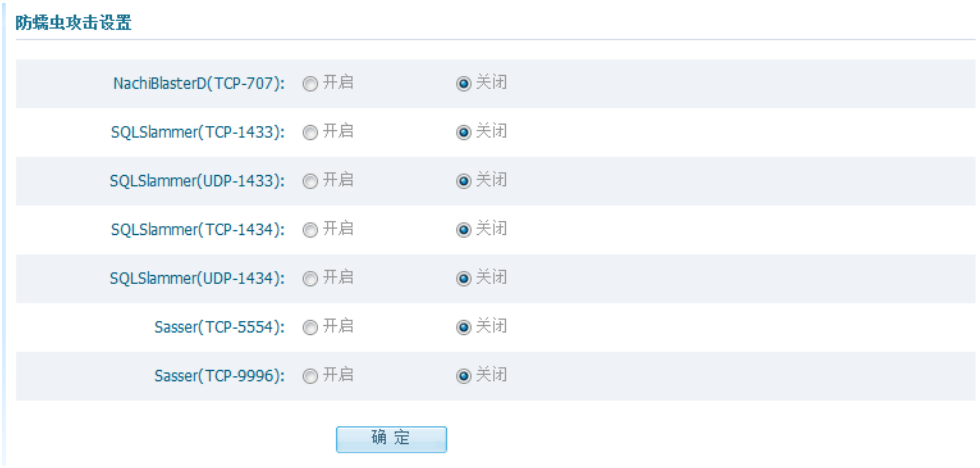
4.11.5. ARP 自动绑定



图片 4-79

对绑定的不信任端口进行 ARP/IP Filter，建立和维护一张 dhcp-snooping 的绑定表，这张表一是通过 dhcp ack 包中的 ip 和 mac 地址生成的，二是可以手工指定。这张表是后续 DAI（dynamic arp inspect）和 IP Source Guard 基础。这两种类似的技术，是通过这张表来判定 ip 或者 mac 地址是否合法，来限制用户连接到网络的。

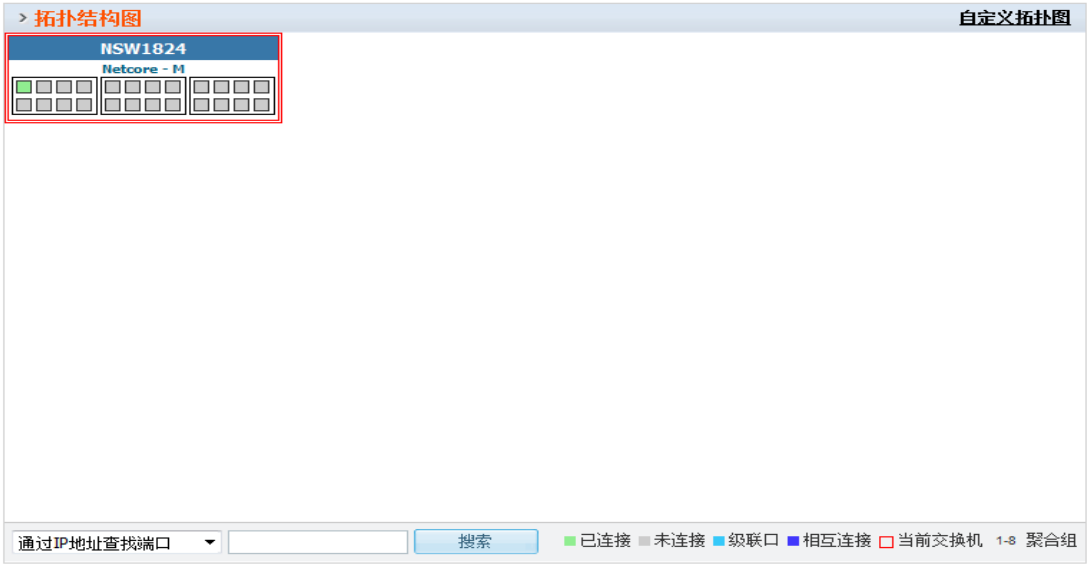
4.11.6. 防蠕虫攻击



图片 4-80

通过对特殊的报文开启放蠕虫攻击，可以有效的防止蠕虫攻击，默认关闭。

4.12. 拓扑结构图



图片 4-81

显示整个联动管理系统里所有交换机设备的网络连接状态的拓扑图

5. 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

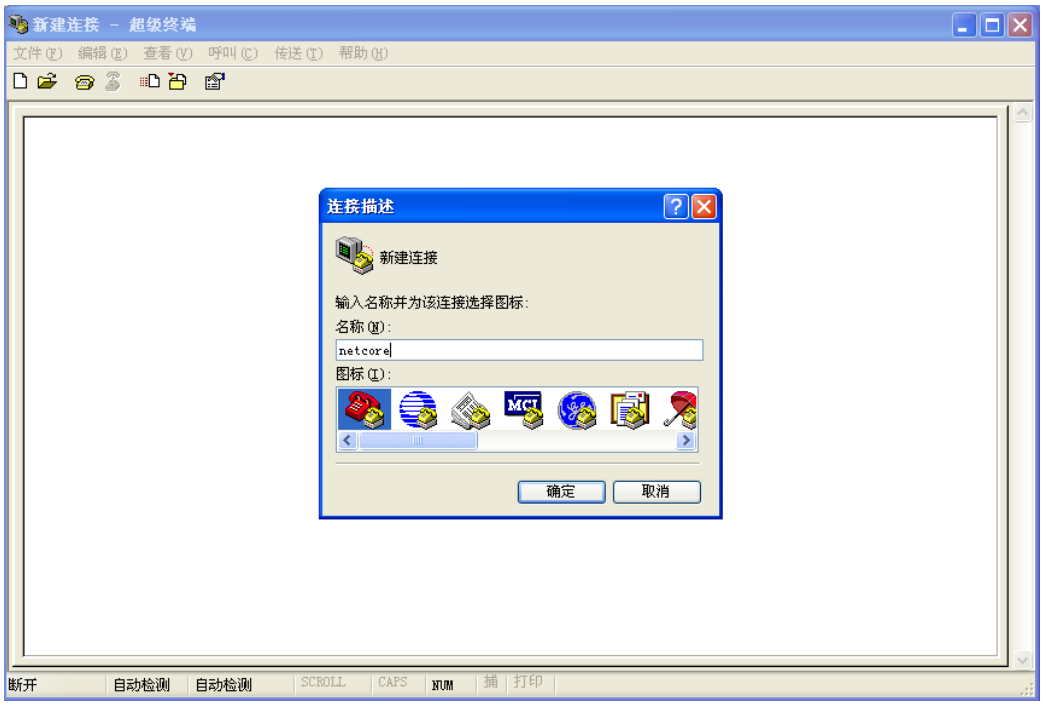
注：此 CONSOLE 管理只用于 X-MODEM 升级和恢复默认参数

5.1. 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

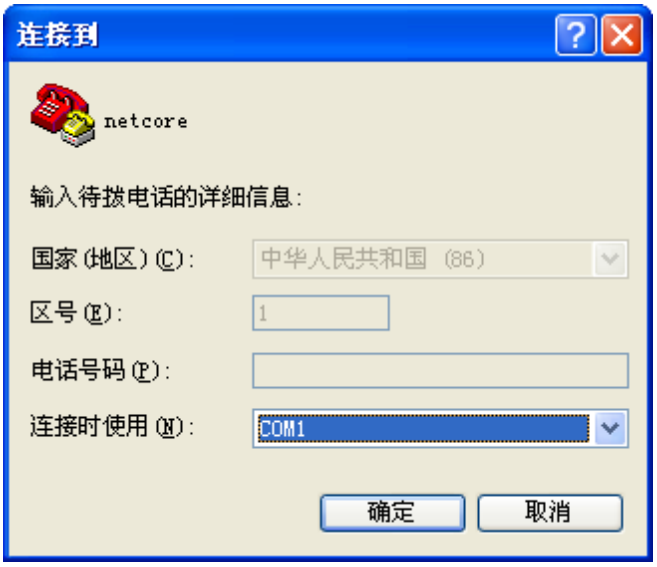
图片 5-1

2、输入超级终端名称，点击确定



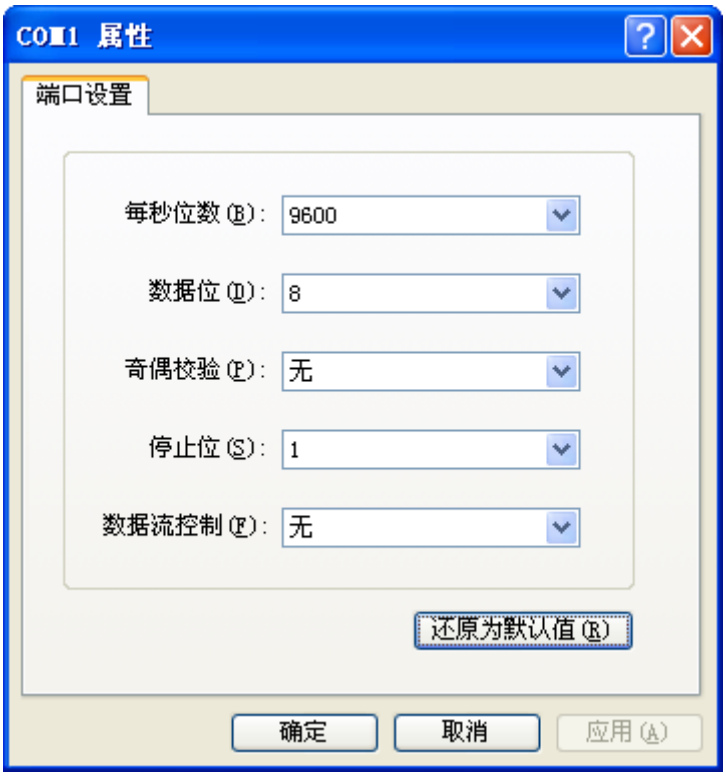
图片 5-2

3、选择连接时使用的端口，点击确定



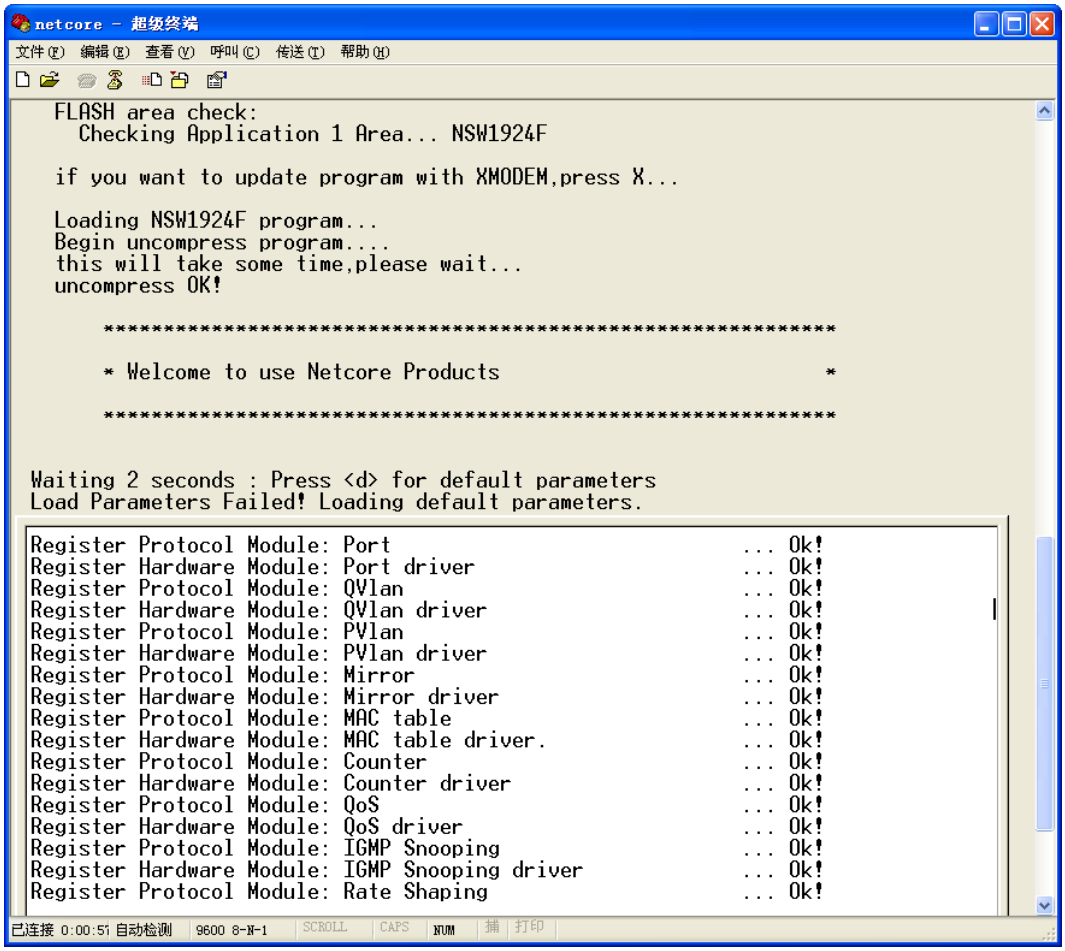
图片 5-3

4、参照下图设置串口属性，点击确定



图片 5-4

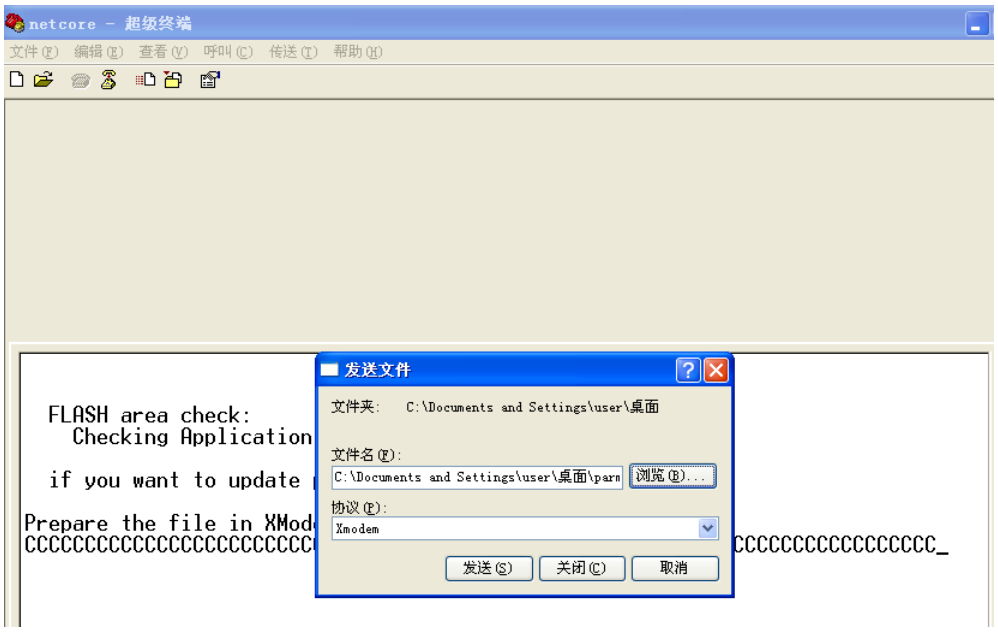
5、将 NSW1824CF 通电，此时按住键盘上“D”不放，恢复成功后超级终端窗口内会显示恢复默认的信息，恢复成功，如下图



图片 5-5

5.2. 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 5-6

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.
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
modem received ok.
md5 check OK.write flash.
update complete! Reset your device.
Reset Your System.
```

图片 5-7

6. 疑难解答

1、链路状态指示灯显示不正常（Link-Error）

- 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；
- 检查连接电缆及两端的 RJ45 接头是否有锈蚀或损坏；
- 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：

- 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；
- 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、无法登录管理交换机

请按照下面的步骤对 NSW1824CF 进行检查：

- 检查 NSW1824CF 是否上电；
- 检查有无链路故障；
- 使用 PING 程序检测 NSW1824CF 有无回应：如果没有回应，则检查 NSW1824CF 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 NSW1824CF 进行检查：

- 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；
- 检查 NSW1824CF 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 NSW1824CF 的 IP 地址设置；
- 检查 PC 和 NSW1824CF 的 IP 地址是否被其它设备占用；

检查登录帐号

- 用户使用 WEB 方式登录时，如果 NSW1824CF 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：

- 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；

- 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；
- 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；
- 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 NSW1824CF 的连接是否稳定可靠。

net·core 磊科

保修卡

客户送修

客户送修

客户送修

尊敬的客户，真诚地感谢您购买NETCORE产品，谨致谢意！
为了保障您的权益，请您仔细阅读以下内容：

包换、保修内容：

- 包换、保修的范围仅限于产品主机，包装及各种连接线、软件、技术资料等附件不在包换、保修的范围内。若产品购买后的一月内出现质量问题，且外观无划伤，可直接更换新产品；
- 对于出现质量问题的产品，若购买超出一月属于保修期限内，换货为良品，不保证为新品；
- 对于在保修范围内出现问题的产品，该型号若不再生产，我司将以升级或替的产品 ，为客户提供免费保换或保修服务：
- 外置电源的保修期为三个月。如果客户返回的电源有明显的硬物损伤、裂痕、断脚、严重变形、电源线破损、断线、裸芯等现象则不予保修，用户可另行购买。
- 保修日期从购买之日起，请您带好相应的购买凭证、保修证书并与代理商所贴保修标签日期相吻合。当您不能出示以上证明时，该产品的免费保修将自其生产日期开始计算。

下列情况不属于免费保换保修范围：

- 未按使用说明书要求安装或使用造成产品损坏；
- 产品超过保换、保修期限；
- 产品序列号被涂改、删除；
- 产品经过非我公司授权人员修理或拆装；
- 客户发回返修途中由于运输、装卸等造成的损坏；
- 产品因意外因素或人为行为而损坏的，如输入不合适的电压、遭受雷击、高温、进水、机械破坏、摔坏、产品严重氧化或生锈等；产品因不可抗拒的自然力量
  如地震、火灾等造成的损坏。

产品售后服务：

- 您可以登陆我公司网站www.netcoretec.com查阅产品信息和下载最新驱动程序，也可以进入论坛和工程师商讨网络技术，或者发送电子邮件到support@netcoretec.com联络技术工程师。
- 您还可以通过全国免费技术支持电话400-8101616联络我公司技术人员。
- 我公司各地办事处也将为您提供产品售后服务

用户反馈（请填写以下资料，并寄回我公司）

产品型号：_____ 产品序列号：_____

经销商名称：_____ 经销商电话：_____

用户名称：_____ 购买日期：_____

通信地址：_____

邮编：_____ 电话：_____

全国分公司联系方式：

北京办事处
电话：010-51665765
010-51297021
上海办事处
电话：021-64683223
021-64683269
沈阳办事处
电话：024-31281515
西安办事处
电话：029-87671238
广州办事处
电话：020-87536936
020-87516989
020-87597503
020-87561836
020-87561836
电话：13998488160
南京办事处
电话：025-86883063
025-83216820
郑州办事处
电话：0371-63897160
0371-63897150
济南办事处
电话：0531-82395855
0531-82395856
杭州办事处
电话：0571-56770679
深圳办事处
电话：0755-82789097
长沙办事处
电话：0731-84137395
哈尔滨办事处
电话：0451-87571848
长春办事处
电话：0431-82777420
武汉办事处
电话：027-68779722

全国技术支持热线
400-810-1616

www.netcoretec.com

制造商：深圳市磊科实业有限公司
地址：深圳市南山区科技园北区新西路2号东方信息港2栋4-5层

PKUM05434