Mexon 兆越®

网管型交换机系列

安装手册

第三版

上海兆越通讯技术有限公司

目录

前　　言

版本说明

本手册版本号为：第三版

内容简介

本手册介绍了网管型工业以太网交换机的性能特点和安装使用方法。请您务必在使用前仔细阅读该产品的所有资料，并按照使用手册中的各项说明来安装和使用该产品，以避免因误操作而损坏设备。

版权声明

免责声明

本手册依据兆越公司的技术资料和现有信息制作其内容，如有更改恕不另行通知。我公司在编写该手册时尽最大努力完善并保证其内容的准确性和可靠性，但我公司不对该手册中的遗漏、不准确或不完善而导致的损失和损害承担责任。

环境保护

本产品的存放、使用和弃置应按照国家相关法律、法规的要求进行。

感谢您使用我们的产品，非常欢迎您对我们的工作提出批评和改善的建议，我们将竭诚为您服务。

第一章 配置管理型交换机

管理型系列交换机通过 Web 可以被访问、配置和管理，在进行这些操作之前，必须通过超级终端设置管理型系列交换机的 IP 地址，或通过更改与之相连 PC 的 IP 地址，才可以访问 Web 页面。接下来本手册会逐步介绍这些操作的详细步骤。

1.1 通过改变 PC 的 IP 地址来设置交换机的 IP 地址

通过 Web 来访问交换机，交换机和 PC 的 IP 必须在同一个局域网络当中。修改 PC 的 IP 地址，确保它和交换机的 IP 同在一个局域网络中，请参考如下的操作步骤：

- 控制面板->网络连接->本地连接->属性->Internet 协议（TCP/IP）
- 管理型系列交换机默认的 IP 地址是：192.168.1.253。设置 PC 的 IP 地址为：192.168.1.X（X 是除 253 外的任一值）。
- 更改 PC 的 IP 地址后，便可用默认的 IP 地址：192.168.1.253，通过 Web 浏览器访问交换机并对其进行相关的配置操作。
- 具体的 Windows 系统操作页面如下：

注意：

该配置示例中没有使用最后一个图片中的高级按钮。使用 IP 地址的高级配置功能，可以让同一个网卡使用多个 IP 伪地址。这样在不改变原先地址的情况依然可以访问交换机设

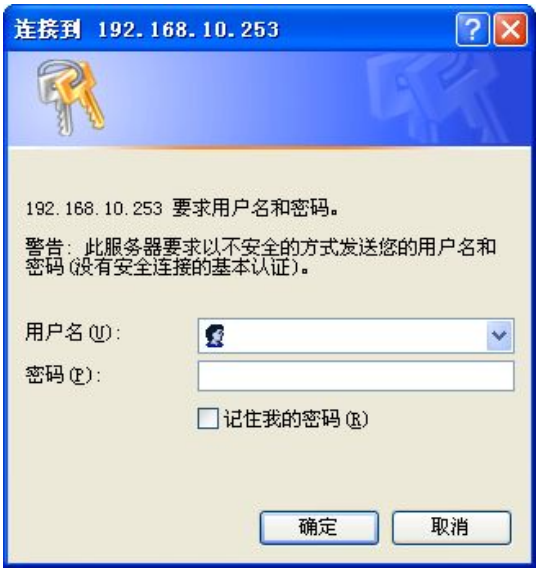
备。但是在 IGMP 轮询和 IEEE 802.1X 轮询中 windows 系统不能正确处理，类 Unix 系统没有这样的问题。请高级使用者务必注意这样的问题。

第二章 Web 管理功能

管理型系列交换机的 Web Server 为访问和配置交换机提供一种便利的方式。大多数内建的网络管理和监控功能可以通过 Web 页面进行编辑和配置。用户可以使用 Internet Explorer 或其他浏览器来访问交换机。打开一个浏览器并在地址栏里输入交换机的 IP 地址，例如：“http://192.168.1.253”，按回车键建立访问连接。接下来将详细的解释如何访问交换机及其丰富功能特性。

2.1 如何登录到 Web Server

打开浏览器，在地址栏里输入交换机的默认 IP 地址，敲击回车键之后，弹出如下的窗体，提示用户输入用户名和密码。默认的用户名和密码都是“admin”。如果用户名或密码输入不正确，该管理型系列交换机的 WebServer 将提供三次机会输入用户名和密码，如果三次输入错误，浏览器显示“401 Unauthorized”错误信息。输入正确的用户名和密码，登录到 WebServer 后，推荐修改用户名和密码。如果您遇到其他更多的问题，可以联系本公司客服中心。



系统自带的用户密码是“admin:admin”，本系列严格区分大小。默认的用户密码是具有管理员权限。

2.2 系统状态

设备状态

- CPU 使用： 当前 CPU 使用的资源占用率
- 内存使用： 系统中已使用的内存大小

当端口连接正常时端口序列号背景色显示为绿色，连接不好或者没有连接时背景色为黑色。

设备信息

注 意：

- 设备中当前时间显示为 1970 年以前的时间，请检查"时间配置"的内容
- 启用了 NTP，但时间仍然显示为 1970 年以前的时间，请使用"网络诊断"中 ping 外网域名确认"设备地址"网关配置正确
- 端口插上后序列号背景色不显示绿色，请检查是否在"端口设置"中禁用该端口，然后再检查网线是否正常
- 发现丢包率大于零，先到"接收帧统计"确认端口，再到"端口设置"中检查是否打开流控。流控打开仍然丢包先检查接口处是否干净，最后检查网线。流控不打开，超过端口速率限制才可以丢包，否则仍是物理连接器件的问题

2.3 端口配置

2.3.1 端口设置

端口号	接口类型	速率模式	双工模式	端口启用	流量控制	极线变换
1	电口	自动协商	全双工	☑	☑	自动翻转
2	电口	自动协商	全双工	☑	☑	自动翻转
3	电口	自动协商	全双工	☑	☑	自动翻转
4	电口	自动协商	全双工	☑	☑	自动翻转
5	电口	自动协商	全双工	☑	☑	自动翻转
6	电口	自动协商	全双工	☑	☑	自动翻转
7	电口	自动协商	全双工	☑	☑	自动翻转
8	电口	自动协商	全双工	☑	☑	自动翻转
G1	SFP	自动协商	全双工	☑	☑	自动翻转
G2	SFP	自动协商	全双工	☑	☑	自动翻转

电口

这种接口就是我们现在最常见的网络设备 RJ-45 接口，俗称"水晶头"，专业术语为 RJ-45 连接器，属于双绞线以太网接口类型。RJ-45 插头只能沿固定方向插入，设有一个塑料弹片与 RJ-45 插槽卡住以防止脱落。

这种接口在 10Base-T 以太网、100Base-TX 以太网以太网中都可以使用，传输介质都是双绞线，不过根据带宽的不同对介质也有不同的要求。

SFP

为 SFP 模块的接口。

速率模式

端口速率表示端口的连接速度，设备共有十兆、百兆、自适应三种速度类型。一共支持如下几种硬件协议：十兆使用 10base-T 互相连接。10base-T 是 1990 年由 IEEE 新认可的，编号为 IEEE802.3，T 表示采用双绞线，现 10BASE－T 采用的是无屏蔽双绞线。当端口使用十兆相连时,ACT 灯（绿色）随数据的通过不停闪烁，而 10M/100M 的状态灯（橙色）保持常灭，SFP 模块的端口速率强制为自动协商。

百兆使用 100base-TX 互相连接。100base-TX 是 IEEE 802.3u 标准，它制定了在五类无屏蔽双绞线（UTP）或屏蔽双绞线（STP）上速率达 100Mbps 的快速以太网信令标准。当端口使用百兆相连时,ACT 灯(绿色)随着数据的通过不停闪烁，而 10M/100M 的状态灯（橙色）保持常亮。

端口启用

该选项提供一个从物理器件上使用/禁用端口的一个可能。当选择禁用端口时，设备从物理上切断了该端口的电源控制，即使有其他设备使用连接线连接，端口所有状态灯都保

持常灭的状态。只有在启用该端口时，所有设备中关于该端口的设置才能生效。该选项提供了一种物理安全机制以保证端口不被非法使用，不可以所有端口都处于禁用状态。

双工模式

交换机的全双工是指交换机在发送数据的同时也能够接收数据，两者同步进行，所谓半双工就是指一个时间段内只有一个动作发生。一般情况下选择为速率选择为″自动协商″即可，这样每个端口都能自动判断与之相连接的设备所能提供的连接方式，并自动调整与之相适应的连接方式，保持最大限度的兼容性。

端口速率处于自动协商时，端口的双工模式也强制处于自动协商模式，只有在强制端口速率时，才能选择端口的双工模式。

流量控制

流量控制用于防止在端口阻塞的情况下丢帧，这种方法是当发送或接收缓冲区开始溢出时通过将阻塞信号发送回源地址实现的。把流经端口的异常流量限制在一定的范围内。流量控制可以有效的防止由于网络中瞬间的大量数据对网络带来的冲击，保证用户网络高效而稳定的运行。

两种控制流量的方式：

1. 在半双工方式下，流量控制是通过背压（backpressure）即我们通常说的背压计数实现的，这种计数是通过向发送源发送 jamming(堵塞)信号使得信息源降低发送速度。

2. 在全双工方式下，流量控制一般遵循 IEEE 802.3X 标准，是由交换机向信息源发送″pause(暂停)″帧令其暂停发送。

采用流量控制，使传送和接受节点间数据流量得到控制，可以防止数据包丢失。当关闭流量控制时使用更上层的协议来控制多台设备之间的连接速率，超过端口转发 限制的数据将直接被丢弃。关闭流量控制常见于设备自身使用低成本或版本过老，不完全支持标准以太网协议的网卡以及使用非标准连接线的场合。

当网卡不能支持暂停帧时、多个网卡与上连端口速率超过 100M 或某个指定的速率时，就会出现设备之间只能以极低的速率在进行通信。此时关闭端口之间的流量控制，设备的通信速率将能够恢复到用户可以接收的速率。同样情况也会发生在使用非标准连接线或

者质量较差的连接线，此时通过关闭流量控制而忽略控制信号。 这样设备可以特定的情况下获得较高的通信速率。

极性变化（ MDI/MDIX 自动适应）

MDI-II(Medium Dependent Interface- II mode)，平行模式介质相关接口,是 IEEE 为了快速以太网 100BASE-T 的 RJ-45 UTP 缆线所制定的标准。II 代表平行配置。MDI-X(Media Dependent Interface-x mode)交叉模式介质相关接口 （非级联口、普通口），与 MDI-II 都是 IEEE 为了以太网络 RJ-45 UTP 缆线所制定的标准。X 代表交错配置 (crossover)。自适应 MDI/MDI-X 功能允许用户使用任何类型的网线(直通网线或交叉网线)来连接 eds 和其它的网络设备，不需要关心连接所使用的网线本身。

当禁用该端口时，任何使用该端口的网线均无法检测到物理连接。只有启用端口时针对该端口的速率、双工、流控才会起作用。目前版本上不支持线序的配置，免得错误的配置导致技术人员无法准确的定位问题。选择自动协商时，速率、双工、流控全部自动协商获得。只有选择固定速率时双工、流控才属于可以配置的项目。千兆不允许使用固定速率配置用于方便与各种厂家的设备相互连接，以免千兆属性配置错误导致无法通信。

2.3.2 带宽管理

提供基于端口速度限制，包括入口和出口速度限制。用户能够限制每个端口的通讯流量或取消端口流量限制。用户能够选择一个固定的速度，端口限制的类型包括所有的单播包、多播包和广播包，当端口达到指定速率时，设备会根据是否启用流控来决定是丢弃该报文还是使用流量控制来限制对端设备的发送速度或接收速度。

提供两个方向的速率限制，其中入口速度是指从 PC 等其他设备流向交换机端口的实际速度。出口速度是指交换机端口流向使用设备之间的实际速度。如果同时限制了两个设备连接端口之间的入口速度和出口速度，则实际的速度为两者中较小的数值。

例如：端口 1 只限制了入口速度，那该端口的通信最大速度就是 10M。同样端口 2 只限制了出口速度，那该端口的通信最大速度就是 9M。

注意：

- 使用端口限速时，流控应该被启用，否则设备之间的速度将不再是平稳曲线
- 使用端口限速时，不应该丢包，除非流控被禁用。丢包的表象是传递速度忽快忽慢
- 端口限速对网线质量要求较高，否则将出现大量的冲突包和破碎的包。

2.3.3 广播风暴抑制

广播风暴

当主机系统响应一个在网上不断循环的报文分组或者试图响应一个没有应答的系统时就会发生广播风暴。一般为了改变这种状态，请求或者响应分组源源不断地产生出来，常使情况变得更糟。随着网络上分组数目的增加，拥塞会随之出现，从而降低网络的性能以至于使之陷入瘫痪。早期对于广播风暴来说就是产生滚雪球效应并产生网络阻塞的故障，而现在多数是由于持续发生的大量广播而造成的网络阻塞或瘫痪，既为广播风暴。导致广播风暴的原因是多样的，例如，在交换机之间，一个冗余或不正确的连接，形成环路，广播包和多播包通过交换机转发到其他端口，收到广播包和多播包的端口将继续循环广播，从而在网络中形成广播风暴。某些情况，广播风暴控制能阻止有人恶意攻击，例如：DOS（Denial of Service）攻击，DOS 通过一台主机向一个广播地址发送 ICMP 请求，导致其他主机回应这个广播地址，从而由于 DOS 攻击产生广播风暴。

针对广播风暴的类型，我们设备检测三种类型的广播报文：

- 广播数据包：目的地址为 FF-FF-FF-FF-FF-FF 的数据帧
- 组播报文：目的地址为 01 开头的数据帧
- 未知单播帧：该数据帧的 MAC 地址不存在设备的内部索引表中，需要向所有端口转发，包括多播和单播流量。

例如：端口 1 只设置了抑制类型为广播抑制、组播抑制和未知单播抑制三种，抑制速率为 10M。出现“设置成功”红色字体，即为成功启用了广播风暴抑制功能。

注意：

- 广播风暴抑制要求端口输入速率不能超过其最大物理带宽，即百兆端口的速率合理速率范围应在 1 至 100M 之间，千兆端口应在 1 至 1000M 之间，且输入的必须是正整数。
- 广播风暴抑制速率对应不同帧长和带有不同校验位的数据包会有一定的数据宽位；比如，64 位帧长的数据设置 10M 抑制速率，但实际测试仪器显示抑制速率为 12M 至 13M，属于正常现象。

2.4 二层特性

2.4.1 QoS 设置

QoS（Quality of Service，服务质量）是各种存在服务供需关系的场合中普遍存在的概念，它评估服务方满足客户服务需求的能力。评估通常不是精确的评分，而是注重分析在什么条件下服务是好的，在什么情况下还存在着不足，以便有针对性地做出改进。在 Internet 中，QoS 所评估的就是网络转发分组的服务能力。由于网络提供的服务是多样的，因此对 QoS 的评估可以基于不同方面。通常所说的 QoS，是对分组转发过程中为延迟、抖动、丢包率等核心需求提供支持的服务能力的评估。

QoS 功能提供 4 个内部队列，每个队列支持 4 个不同等级的通讯量，高优先权的数据包在交换机里暂留的时间较短，对某些延迟敏感的通信量支持较低的潜伏期。根据端口 ID、MAC 地址、802.1p 优先级标签、DiONetServ 和 IP TOS，设备能够对数据包分类到某个相应的等级。

IEEE 802.1P:流量优先级

802.1P 协议头包括一个 3 位优先级字段，该字段支持将数据包分组为各种流量种类。802.1P 是 IEEE 802.1Q (VLAN 标签技术)标准的扩充协议，它们协同工作。IEEE 802.1Q 标准定义了为以太网 MAC 帧添加的标签。VLAN 标签有两部分：VLAN ID （12 比特）和优先级（3 比特）。IEEE 802.1Q VLAN 标准中没有定义和使用优先级字段，而 802.1P 中则定义了该字段。802.1P 中定义的优先级有 8 种，最高优先级为 7，应用于关键性网络流量。优先级 6 和 5 主要用于延迟敏感（delay-sensitive）应用程序。优先级 4 到 1 主要用于受控负载（controlled-load）应用程序，如流式多媒体和关键性业务流量。

优先级 0 是缺省值，并在没有设置其它优先级值的情况下自动启用。设备默认设置中优先级 0 和优先级 1 映射到第一队列，即优先级最差的队列。优先级 2 和优先级 3 映射到第二队列，优先级 4 和优先级 5 映射到第三队列，优先级 6 和优先级 7 映射到最快队列即优先级最高的队列。

基于端口的流量优先级

设备中基于端口的优先级只定义了两组，如果使用最快队列，则所有从该端口进入的数据包从各个端口转发出去的时候拥有绝对的优先权。否则在转发时需要再判断 IEEE 802.1P 和区分服务（DiffServ）优先级。


端口优先级配置：

端口号	优先级	端口号	优先级	端口号	优先级	端口号	优先级
1	第一队列	2	第一队列	3	第一队列	4	第一队列
5	第一队列	6	第一队列	7	第一队列	8	第一队列
G1	第一队列	G2	第一队列				

2.4.2 虚拟局域网(VLAN)

VLAN 技术允许网络管理者将一个物理的 LAN 逻辑地划分成不同的广播域（或称虚拟 LAN，即 VLAN），每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。但由于它是逻辑地而不是物理地划分，所以同一个 VLAN 内的各个工作站不被放置在同一个物理空间里，即这些工作站不一定属于同一个物理 LAN 网段。一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，即使是两台计算机有着同样的网段，但是它们却没有相同的 VLAN 号，它们各自的广播流也不会相互转发,从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

支持基于端口的 VLAN,提供跨越交换机的 VLAN 和不跨越交换机的 VLAN 的两种设置。跨越交换机的 VLAN 遵循标准的 IEEE802.1Q 协议，而 IEEE 802.1Q 规范为标识带有 VLAN 成员信息的以太帧建立了一种标准方法。IEEE 802.1Q 标准定义了 VLAN 网桥操作，从而允许在桥接局域网结构中实现定义、运行以及管理 VLAN 拓朴结构等操作。 802.1Q 标准主要用来解决如何将大型网络划分为多个小网络，如此广播和组播流量就不会占据更多带宽的问题。

VLAN 类型

基于端口的 VLAN

端口 VLAN 提供了一个能够把交换机端口划分到不同的虚拟私有域里去的解决方案。在不同的私有域之间，是不允许进行数据交换的，所以各私有域里的数据维护变得相对安全。关于端口 VLAN，使用不同的标识来区分不同的 VLAN。使用相同的 ID 标识将导致内部的成员组被替换，新的 ID 标识将建立新的转发规则，所有的端口必须属于一个或者多个 VLAN。

1、添加表项

组名称在端口 VLAN 中可以使用任意有效字符，基于端口的 VLAN 纯粹是修改内部的转发规则，因此无法跨越交换机实现。

2、删除表项

将存在的转发项从内部的表项中删除。

如上图的例子中我们所有的端口放在同一个 VLAN 之中，每个端口之间都可以互相通信。可以删除默认的配置，使用不同的名字增加一些选项。组内的端口之间可以通信，而组外的端口是不可以相互通信的。可以配置多个端口属于多个 VLAN。

3、保存配置

将配置保存，如不保存当前配置，则基于端口 VLAN 划分的配置不会生效。

IEEE 802.1Q VLAN

IEEE 802.1Q 完成 VLAN 功能的关键在于其 VLAN 标签。一个包含 VLAN 信息的标签字段可以插入到以太帧中，设备将根据内建的转发规则处理数据的转发，同时根据内建的剥离规则决定是否将出去的数据中的 VLAN 标签剥离。数据帧中 VLAN 标记协议标识字段为 2 个字节，数值为 0x8100。

1、添加表项

IEEE 802.1Q 中 VID 必须使用纯粹数字，其范围为 1-4094，VID 表示为默认端口 VID，相当为 PVID 的概念。

2、删除表项

将存在的转发项从内部的表项中删除。

如果将所有的端口放在同一个 VLAN 之中，每个端口之间都可以互相通信。可以删除默认的配置，使用不同的 VID 增加一些选项。组内的端口之间可以通信，而组外的端口是不可以相互通信的。值得注意是如果该端口属于多个 VLAN 的话，则配置该端口为 trunk 端口，加入到所属 VLAN 内。

VLAN 配置

启用灵活的 IEEE 802.1Q 设置

- 端口默认 VID：端口默认的 VID 标识
- TRUNK 端口列表：默认所有端口都不属于 trunk 端口，勾选该端口后，该端口角色即为 trunk 端口
- VID 值：端口的 VLAN ID
- 端口列表：选定该端口后，该端口就属于 VID 所在 VLAN
- GVRP：启用 GVRP 协议后，端口会根据 GVRP 的消息，动态创建 VLAN

2.4.3 动态组播

IGMP 侦听

通过侦听主机向路由器的 IGMP 成员报告消息的方式，形成组成员和交换机接口的对应关系；交换机根据该对应关系将收到组播数据包只转给具有组成员的接口。

IGMP 查询

开启 IGMP 查询功能，在没有路由器或者路由器不支持组播的情况下扮演 IGMP 组播协议的状态机维护角色（暂不支持查询器自动选举功能，需强制指定）。

IGMP 查询间隔

开启 IGMP Qurey 功能后，定期向本网段内发送普遍组查询报文（224.0.0.1）的周期。只有在 IGMP 查询功能启用后，才能配置查询间隔时间。

组成员生存时间

当一个端口动态加入某组播组时，交换机为该端口启动一个定时器，其超时时间就是动态成员端口老化时间。

动态路由端口生存时间

动态路由端口表示连接组播路由器的端口，也就是发送 query 查询报文的设备，交换机接收到 igmp report 报文或者 leave 报文，则会向路由端口转发。当一个端口接收到普遍组查询报文时，端口将变为动态路由端口，交换机为该端口启动一个定时器，其超时时间就是动态路由端口老化时间。

静态路由端口

将端口配置为静态路由端口，该端口将始终保持为路由端口角色。

GMRP

通过侦听主机发送的 gmrp join 和 leave 成员报告消息的方式，形成组成员和交换机接口的对应关系；交换机根据该对应关系将收到组播数据包只转给具有组成员的接口。

GMRP 协议的相关参数，均为默认，用户不能进行配置。

2.4.4 静态多播转发表

提供静态 MAC 地址转发功能。目的地址包含静态 MAC 地址的数据包将会被转发到指定的端口。内建在交换机芯片里的转发地址表，不仅保持学习功能。静态 MAC 地址履行转发功能，但是它不受老化处理的支配。

按钮"增加"、"修改"和"删除"用来添加、修改和删除静态 MAC 地址。静态 MAC 地址域（Static MAC Address）从用户请求一个有效的输入，如果输入是一个无效的 MAC 地址，将弹出消息警告。端口域用来选择静态 MAC 地址转发端口，可以指定一个或多个转发端口。点击"增加"、"修改"和"删除"后将触发静态 MAC 地址转发表的更新。

如输入示例中，加入地址“01-00-5E-36-42-01”成员为端口 1，2。所有非多播地址在该表项中是不允许被加入的。输入必须类似于“静态组播 MAC 地址”表格中的内容相似，同时我们也支持“01:00:5E:36:42:04”和“01005E364204”这两种格式，以提供客户在方便的时候提供“拷贝”和“粘贴”功能。

注意：

- 这个功能对网络转发多播影响很大，除非你确认添加的地址没有问题，否则请慎用
- 下面的多播地址为设备或协议保留，请不要使用：
- 0180C20000xx
- 01005E0000xx
- IGMP 动态学习将不会更新静态输入的多播地址，静态多播转发表更多的是一种安全机制

2.5 链路备份

2.5.1 端口汇聚

TRUNK 是端口汇聚的意思，就是通过配置软件的设置，将 2 个或多个物理端口组合在一起成为一条逻辑的路径从而增加在交换机和网络节点之间的带宽，将属于这几个端口的带宽合并，给端口提供一个几倍于独立端口的独享的高带宽。Trunk 是一种封装技术，它是一条点到点的链路，链路的两端可以都是交换机，也可以是交换机和 路由器，还可以是主机和交换机或路由器。基于端口汇聚（Trunk）功能，允许交换机与交换机、交换机与路由器、主机与交换机或路由器之间通过两个或多个 端口并行连接同时传输以提供更高带宽、更大吞吐量， 大幅度提供整个网络能力。

一般情况下，在没有使用 TRUNK 时，大家都知道，百兆以太网的双绞线的这种传输介质特性决定在两个互连的普通 10/100 交换机的带宽仅为 100M，如果是采用的全双工模式的话，则传输的最大带宽可以达到最大 200M，这样就形成了网络主干和服务器瓶颈。要达到更高的数据传输率，则需要更换 传输媒介，使用千兆光纤或升级成为千兆以太网，这样虽能在带宽上能够达到千兆，但成本却非常昂贵（可能连交换机也需要一块换掉），

更本不适合低成本的中小 企业和学校使用。如果使用 TRUNK 技术，把四个端口通过捆绑在一起来达到 800M 带宽，这样可较好的解决了成本和性能的矛盾。

TRUNK（端 口汇聚）是在交换机和网络设备之间比较经济的增加带宽的方法，如服务器、路由器、工作站或其他交换机。这中增加带宽的方法在当单一交换机和节点之间连接不能满足负荷时是比较有效的。 TRUNK 的主要功能就是将多个物理端口（一般为 2－4 个）绑定为一个逻辑的通道，使其工作起来就像一个通道一样。将多个物理链路捆绑在一起后，不但提升了整个网络 的带宽，而且数据还可以同时经由被绑定的多个物理链路传输，具有链路冗余的作用，在网络出现故障或其他原因断开其中一条或多条链路时，剩下的链路还可以工作。

设备一共支持三组 TRUNK 组。

注意：

- TRUNK 组要求所有属性相同，包括速率、双工、STP 等等状态
- 如果你不确认 STP 状态，请关闭 RSTP 功能，或者关闭其他，只留一条 STP 通道

2.5.2 快速环网

快速环网为断开的以太网络提供自动恢复重连机制，在网络中断或网络产生故障时，它有链路冗余、自恢复能力。快速环网专业为高可靠性的工业控制网络应用而开发设计。

交换机每个端口都可以用做环网，与其他交换机相连，快速环网冗余机构启用备份链路，迅速恢复网络通信。

下表参数仅供参考：

冗余技术	快速环网	RSTP	STP
恢复时间	300ms	Up to 5s	Up to 30s

1、快速环网配置

三种状态：启用快速环网、禁用冗余、启用快速生成树，该功能与 RSTP 同样利用生成原理，因此不能同时启用

2、环网序号

网络中用于唯一表明逻辑环网的序号，不同逻辑环网允许使用不同的ＩＤ。

3、组环端口

选择相应的组环端口，自愈环网使用两个端口，双路冗余环网使用一个端口。

4、当前状态

显示当前的环网状态，通过查看状态可以得知环网是否正常。没有启用环网前，状态为尚未启用；配置了环网后如果环网协商状态成功则会显示“master 或 salve”，如果环网协商不成功则会显示状态为“状态未知”。

5、组环端口状态

标明当前的端口状态：转发或阻塞。

2.5.3 快速生成树

生成树的协议是一种二层管理协议，它通过有选择性地阻塞网络冗余链路来达到消除网络二层环路的目的，同时具备链路的备份功能。

由于生成树的协议本身比较小，所以并不像路由协议那样广为人知。但是它却掌管着端口的转发大权-"小树枝抖一抖，上层协议就得另谋生路"。真实情况也确实如此，特别是在和别的协议一起运行的时候，生成树就有可能断了其他协议的报文通路，造成种种奇怪的现象。

STP 协议的基本思想十分简单。大家知道，自然界中生长的树是不会出现环路的，如果网络也能够像一棵树一样生长就不会出现环路。于是，STP 协议中定义了根桥 （Root Bridge）、根端口（Root Port）、指定端口（Designated Port）、路径开销（Path Cost）等概念，目的就在于通过构造一棵自然树的方法达到裁剪冗余环路的目的，同时实现链路备份和路径最优化。用于构造这棵树的算法称为生成树算法 SPA（Spanning Tree Algorithm）。

要实现这些功能，网桥之间必须要进行一些信息的交流，这些信息交流单元就称为配置消息 BPDU（Bridge Protocol Data Unit）。STP BPDU 是一种二层报文，目的 MAC 是多播地址 01-80-C2-00-00-00，所有支持 STP 协议的网桥都会接收并处理收到的 BPDU 报文。该报文 的数据区里携带了用于生成树的计算的所有有用信息。

要了解生成树的协议的工作过程也不难，首先进行根桥的选举。选举的依据是网桥优先级和网桥 MAC 地址组合成的桥 ID（Bridge ID），桥 ID 最小的网桥将成为网络中的根桥。在网络中，各网桥都以默认配置启动，在网桥优先级都一样（默认优先级是 32668）的情况下， MAC 地址最小的网桥成为根桥，例如图 1 中的 SW1，它的所有端口的角色都成为指定端口，进入转发状态。

接下来，其他网桥将各自选择一条 "最粗壮"的树枝作为到根桥的路径，相应端口的角色就成为根端口。假设有交换机 SW2 和 SW1、SW3 之间的链路是千兆 GE 链路，SW1 和 SW3 之间的链路是百兆 FE 链路，SW3 从端口 1 到根桥的路径开销的默认值是 19，而从端口 2 经过 SW2 到根桥的路径开销是 4+4=8，所以端口 2 成为根端口，进入转发 状态。同理，SW2 的端口 2 成为根端口，端口 1 成为指定端口，进入转发状态。

根桥和根端口都确定之后一棵树就生成了，如图中实线所示。下面的任务是裁剪冗余的环路。这个工作是通过阻塞非根桥上相应端口来实现的，例如 SW3 的端口 1 的角色成为禁用端口，进入阻塞状态。

生成树经过一段时间（默认值是 30 秒左右）稳定之后，所有端口要么进入转发状态，要么进入阻塞状态。STP BPDU 仍然会定时从各个网桥的指定端口发出，以维护链路的状态。如果网络拓扑发生变化，生成树就会重新计算，端口状态也会随之改变。

为了解决 STP 协议的这个缺陷，在世纪之初 IEEE 推出了 802.1w 标准，作为对 802.1D 标准的补充。在 IEEE 802.1w 标准里定义了快速生成树协议 RSTP（Rapid Spanning Tree Protocol）。RSTP 协议在 STP 协议基础上做了三点重要改进，使得收敛速度快得多（最快 1 秒以内）。

第一点改进：为根端口和指定端口设置了快速切换用的替换端口（Alternate Port）和备份端口（Backup Port）两种角色，当根端口/指定端口失效的情况下，替换端口/备份端口就会无时延地进入转发状态。图 2 中所有网桥都运行 RSTP 协议，SW1 是根桥， 假设 SW2 的端口 1 是根端口，端口 2 将能够识别这种拓扑结构，成为根端口的替换端口，进入阻塞状态。当端口 1 所在链路失效的情况下，端口 2 就能够立即进入 转发状态，无需等待两倍 Forward Delay 时间。

第二点改进：在只连接了两个交换端口的点对点链路中，指定端口只需与下游网桥进行一次握手就可以无时延地进入转发状态。如果是连接了三个以上网桥的共享链路，下游网桥是不会响应上游指定端口发出的握手请求的，只能等待两倍 Forward Delay 时间进入转发状态。

第三点改进：直接与终端相连而不是把其他网桥相连的端口定义为边缘端口（Edge Port）。边缘端口可以直接进入转发状态，不需要任何延时。由于网桥无法知道端口是否是直接与终端相连，所以需要人工配置。

可见，RSTP 协议相对于 STP 协议的确改进了很多。为了支持这些改进，BPDU 的格式做了一些修改，但 RSTP 协议仍然向下兼容 STP 协议，可以混合组网。

快速生成树的几个概念

- 交换机优先级：作为网桥的优先级，网桥优先级和网桥 MAC 地址组合成的桥 ID，桥 ID 最小的网桥将成为网络中的根桥
- 轮询间隔：多长时间发送一次 BPDU 的数据包
- 转发延迟：指交换机的端口状态在过渡状态下（listening 和 learning）下维持一个 forward delay 的时间
- 最大老化时间：如果在最大老化时间内都没有收到新的 BPDU，非根桥就开始新根桥的选举过程。

快速生成树中端口相关的几个概念

- 端口路径开销：端口链路代价，以太网端口的路径开销与该端口的链路速率有关,链路速率越大应该将该参数配置的越小,当该参数被配置为缺省值时，STP 协议自动检测当前以太网端口的链路速率并换算成相应的路径开销。也可以手动指定端口的路径开销。
- 端口优先级：更改端口优先级来影响生成树端口角色的选举，默认端口优先级为 128，配置端口优先级时以 16 为一个步长。
- 点到点网络连接：交换机端口和交换机端口直连，则该端口就是 P2P 接口。RSTP 针对 P2P 接口采用协商机制，可以实现端口状态的快速转换 。
- 直接连接终端：处于网络边缘的交换机一般与终端设备相连，如 PC 机、工作站。把和这些终端设备相连的端口配置成为 Edge 端口，可以实现端口状态的快速转换，而不需要 Discarding，Learning，Forwarding 的转换过程。

- 不参与生成树结构：不参与生成树的协议的运行 。

生成树中的四个状态:

- 阻塞(Blocking)(可接收 BPDU 数据包,如果期间没收到 BPDU 后转到监听状态)，链路刚接通时端口都处于阻塞状态 。
- 监听 (Listening)(可以接收数据包)，连通之后马上接通时交换机在阻塞状态下停留 max age=20s 的时间，判断交换机的这个端口有没有可能成为根端口或指定端口，如果有可能成为根端口或指定端口的话就把端口的状态转换到 listening(监听,该状态维持 15 秒)状态。期间中收发 BPDU 数据包，完成生成树的根的选举、构造，完成端口状态去向的决定。如果决定是根端口 或指定端口的话就转换到 learning 状态，如不是的话转换到阻塞状态。
- 学习(Learning),停留 forward delay(=15s)时间，继续计算判断端口能不能成为根端口或者指定端口，此时具有学习 MAC 地址的功能。如果决定后转换到转发状态。
- 转发(Forwarding)(可以接收和发送 BPDU 数据包)。如示例中配置，该网桥使用的优先级为“32668”，其与自己的 MAC 形成一个网桥的 ID，如果网络上没有网桥的 ID 小于自己，则自身为根桥。网络中不存在两个完全一样 ID 的网桥。该网桥每隔 2 秒钟向所有的指定端口发送 BPDU 报文，当在最大老化时间 20 秒内没有收到 BPDU 报文认为端口失效，重新计算网桥状态。每个状态之间的切换如果需要变化为转发的话需要等待 15 秒。

2.6 访问控制

2.6.1 用户密码

企业往往要求监控设备的管理员和系统或网络的管理员是两个角色，其权限要分开，即前者只负责监控业务的管理，后者只负责系统或网络的管理。交换机提供的分级管理：用户权限和管理权限。用户权限只有查看交换机状态的权力，而只有系统管理员才可以对交换机的参数进行配置。

用户索引

用户索引，表示哪一组用户。在下拉列表框里共有三个用户索引

访问等级

管理员：对所有设置拥有查看和设置的权限

观察员：对所有设置只有查看的权限

用户名

访问者的标识，允许不大于 16 字节的字母的组合

输入密码

访问者使用的密码，用户权限允许不大于 16 字节的字母的组合

确认密码

确认上次输入的密码是正确的

注意：

1) 如果忘记用户名和密码，请联系公司首页中的技术支持，以便得到帮助

2.6.2 端口隔离

启用端口隔离功能的端口不能和其他端口隔离组内的端口进行通讯，只能和其他普通端口进行访问。

2.6.3 登陆控制

Telnet 登录控制

该功能是针对 Telnet 服务而言，默认 Telnet 服务开启，用户可以通过 telnet client 连接到交换机，如果该功能为禁用状态，则会关闭 Telnet 服务。

登陆 IP 地址控制

这个是设备提供高级的通信过滤功能。这个过滤功能作为防火墙的一个完整部分被使用。通常防火墙是一个网络设备，来控制对网络资源的访问。防火墙应被连接在局域网络的入口点。 当启用这个功能的时候，仅符合条目的计算机才可以访问。

在端口上绑定了条目后，相当于在该端口配置了 ACL 条目，只有符合条目的 IP 地址才能登录交换机(web)。

2.6.4 IEEE 802.1X 端口认证

IEEE 802.1x 的认证体系结构中采用了"可控端口"和"不可控端口"的逻辑功能，从而可以实现业务与认证的分离。用户通过认证后，业务流和认证流实现分离，对后续的数据包处理没有特殊要求，业务可以很灵活，尤其在开展宽带组播等方面的业务有很大的优势，所有业务都不受认证方式限制。

802.1x 结构主要有三部分组成：

- 申请者 supplicant：想得到认证的用户或客户

- 认证服务器 authentication server：典型例子为 RADIUS 服务器
- 认证系统 authenticator：对端间设备，如无线接入点、交换机等

我们设备可以同时扮演认证系统和认证服务器两个角色，也可以使用额外的认证服务器，

定时更新认证

802.1x 的重认证周期时间，用来增强认证的安全性

Radius 服务器远程/本地

设备中内建 Radius 服务器，如果选择内部的 Radius 服务器，申请者将只能使用内部的 Raduis 数据库的用户和密码。如果使用外部的 Radius 服务器则需要填写认证服务器的 IP 地址和端口号。

认证服务器

Radius 远程接入验证服务器,也就是认证用的授权用的，设置的 IP 地址/域名是设备可以访问到的，默认端口是 1812。

认证共享密码值

用于设备访问认证服务器的共享密码字符串

计费服务器设置

计费服务器实现的功能是计费，设置的 IP 地址/域名是设备可以访问到的，默认端口是 1813,如示例中的设置，IEEE 802.1X 服务器每 3600 秒重新认证一次客户端。使用的是本地数据库，本地数据库的介绍如下一章节。客户端使用的 MD5 认证，具体设置如下图：

如果没有发现验证的选项，请按照下文注意事项去操作操作系统。当使用远程 Radius 服务器时，请注意将所有交换机互相连接的端口和与服务器直接连接的端口配置为强制认证，即是禁用“802.1X 认证”。

注意：

- 申请者和认证系统之间使用 MD5-质询，其他方式不支持
- 如果网络连接属性没有"身份验证"选项，请选择"附件"->"管理工具"->"组件服务"->"服务"，设置"Wired AutoConfig"为"自动"
- 计费服务器设置错误同样会导致申请者无法通过身份认证。没有计费服务器就不需要设置
- 所有的上连口或下连口必须强制通过认证，即"禁止使用认证"，否则无法使用远程服务器，除非使用内部认证服务器
- 使用远程服务器时，管理员务必确认设备可以访问远程服务器，即"设备地址"中网关设置正确，如果使用域名则 DNS 必须设置正确

2.6.5 Radius 数据库

RADIUS：远程用户拨号认证系统（RADIUS：Remote Authentication Dial In User Service）

RADIUS 是一种在网络接入服务器（Network Access Server）和共享认证服务器间传输认证、授权和配置信息的协议。 RADIUS 使用 UDP 作为其传输协议。此外 RADIUS 也负责传送网络接入服务器和共享计费服务器间的计费信息。

这里的数据库只作为认证、授权的一部分，任何申请者的用户名和密码吻合数据库的匹配规则时，设备的认证系统即授权于该申请者。

按钮"增加"和"删除"用来添加、修改和删除用户组。登陆帐户是一个不大于 16 字节的数字、字母和汉字的组合， 用户密码也是是一个不大于 16 字节的数字、字母和汉字的组合。点击"增加"是已存在的用户名将导致使用新的密码，新的用户名将增加一个新的用户组。"删除"将去除光标所指的用户组。点击"保存设置"将触发数据库的更新和整个认证的重新开始。

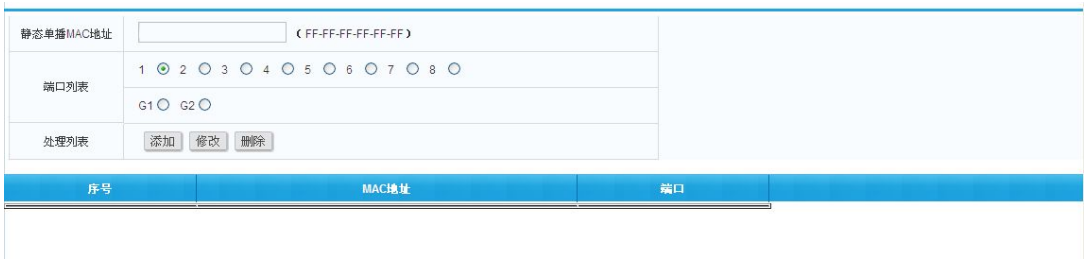
注意：

- 不启用本地 Radius 认证，该数据库内容实际上是无效的

2.6.6 静态 MAC 地址端口锁定

静态地址表

静态 MAC 地址区别与一般的由学习得到的动态 MAC 地址。静态地址一旦被加入，该地址在删除之前将一直有效，不受最大老化时间的限制。静态地址表记录了端口的静态地址。静态地址表中一个 MAC 地址对应一个端口，如果设置，则所有发给这个地址的数据只会转发给该端口。



按钮"增加"、"修改"和"删除"用来添加、修改和删除静态 MAC 地址。静态 MAC 地址域（Static MAC Address）从用户请求一个有效的输入，如果输入是一个无效的 MAC 地址，将弹出消息警告。端口域用来选择静态 MAC 地址转发端口，可以指定一个或多个转发端口。点击"增加"、"修改"和"删除"后将触发静态 MAC 地址转发表的更新。

注意：

- 这个功能是一种安全机制，请谨慎确认设置，否则请慎用
- 请不要使用多播地址作为输入地址
- 请不要输入保留的 MAC 地址，如本机的 MAC 地址

2.7 远程监控

2.7.1 SNMP 管理

简单网络管理协议（SNMP）由 Internet 工程任务组定义，是组成 Internet 协议的一部分。在想关注某台网络设备的条件下，使用 SNMP 通过网络管理系统来监控网络设备。SNMP 协议由一系列标准网络管理、应用层协议、数据库、数据对象组成。SNMP 协议能够通过管理系统的窗体，显示管理数，如系统描述配置。这些配置描述可以通过一个支持 SNMP 的管理应用程序进行查询或设置。

设备支持 SNMP V1/V2c。SNMP V1 和 V2c 都使用公有字符串进行匹配认证，这意味着使用公有或私有字符串，SNMP 服务器允许只读方式或读写方式访问所有对象。

基于 TCP/IP 协议，SNMP 通常使用 UDP 端口 161（SNMP）和 162（SNMP-traps），SNMP 协议代理存在于网络设备里，使用 MIBs（information specific to the device）作为设备接口，通过代理，这些网络设备可以被监控或控制。当一个 trap 事件发生时，消息被 SNMP Trap 传输，此时，一个可用的 trap 接收器可以收到这个 trap 消息。

SNMPV1、SNMPV2C 采用团体名认证。SNMP 团体（Community）用一个字符串来命名，称为团体名（Community Name）。SNMP 团体名用来定义 SNMP manager 和 SNMP agent 的关系。团体名起到了类似于密码的作用，可以限制 SNMP manager 访问以太网交换机上的 SNMP agent。

SNMP 一共支持三种基本操作：

- Get 操作：管理者使用该操作查询 Agent 的某个变量的值
- Set 操作：管理者使用该操作设置 Agent 的某个变量的值
- Trap 操作：Agent 使用该操作像管理者发出异常警报信息

snmp 配置：默认 snmp 服务功能开启，默认版本为 v1。

只读团体名 ：用一个字符串来命名的 SNMP 团体名，该团体只有 Get 操作的权限。

读写团体名 ：用一个字符串来命名的 SNMP 团体名，该团体有 Get 操作和 Set 操作的权限 。

SNMP TRAP 网关 ：Agent 发出异常警报信息的接受者的网络 IP 地址

2.7.2 Email 远程报警

在系统产生报警日志时，将日志消息以邮件的形式发送进行通知。

邮箱服务器：发件服务器

邮箱账户：发送邮件的账户

收件人地址：接收邮件的账户

邮件回复地址：

2.7.2 即时报警

即时告警功能默认启用，点击“复位”按钮，可以重置即时报警功能。

最新告警信息：告警提示信息

告警设置：当进行报警设置时，当实际端口接线符合相应的报警设置时，则会在告警信息栏显示相应的告警信息。

2.8 端口统计

2.8.1 总流量统计

端口	发送总字节	接收总字节	单播包总个数	多播包总个数	广播包总个数	错误包总个数
1	0	0	0	0	0	0
2	3015463	3191715	38467	4286	1258	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
G1	2135	0	0	7	11	0
G2	2135	0	0	7	11	0

端口：显示设备所有端口。

发送总字节：端口发送所有数据包的总字节数目。

接收总字节：端口接收所有数据包的总字节数目。

单播包总个数：端口发送和接收地址为单播地址的数据包的个数 。

多播包总个数：端口发送和接收地址为多播地址的数据包的个数 。

广播包总个数：端口发送和接收地址为广播播地址的数据包的个数 。

错误包总个数：端口发送和接收地址因为各种原因的错误的数据包的个数。

2.8.2 MAC 地址表

MAC（Media Access Control）地址是网络设备的硬件标识，交换机根据 MAC 地址进行报文转发。MAC 地址具有唯一性，这保证了报文的正确转发。 每个交换机都维护着一张 MAC 地址表。在这张表中，MAC 地址和交换机的端口一一对应。当交换机收到数据帧时，根据 MAC 地址表来决定对该数据帧进行过滤还是转发到交换机的相应端口。 MAC 地址表是交换机实现快速转发的基础和前提。

设备 MAC 地址表中的 MAC 地址分为以下三种类型：

1、动态 MAC 地址

动态 MAC 地址是交换机在网络中通过数据帧学习到的，当老化时间到来时会被删除。当设备所连接的交换机的端口发生变化时，MAC 地址表中相应的 MAC 地址和端口的对应关系也会随之改变。 动态 MAC 地址在交换机关电重启后会消失，需要重新学习。

2、静态认证 MAC 地址

静态认证 MAC 地址，通过配置静态的 MAC 地址绑定获得，手动绑定的静态 MAC 地址不做老化处理，在交换机重启之后，也不会消失；而通过配置 IEEE 802.1X 认证后产生的静态 MAC 地址，不会被交换机老化掉。不管设备所连接的交换机的端口发生怎样的变化，MAC 地址表中 MAC 地址和端口的对应关系始终不会改变，其关系完全由 IEEE 802.1X 认证服务器控制，该静态 MAC 地址在交换机关电重启后会消失。

可以选择“自动”和“端口”两种排序类型 。

2.8.3 环回测试

我们在设备端口上启用 loopback 功能使接口从内部将自己发送的信号转接到自己的接收端，通过检 查数据发送和接收的情况来判断端口工作状态是否正常。如果需要对端口进行完全的检测，可以使用符合标准的短跳线将端口收发短接构成环。如果端口正常，可以将线路的一部分或全部包括到环中进行测试，即在线路中的某个点上进行短接构成环。这些点可以是在配线架、CSU/DSU、传输设备等之上。

例如，端口 1 开启环回检测功能，若端口 1 检测到该端口下有环路（即收到从本端口发出的数据）后，交换机会使端口 1 处于受控状态；待环路消失，又能自动恢复使能状态。

注意：

- 对于网络层次较高，环路检测功能作用不大，同时如果误用造成的不良影响可能会很大，因此该环境下的交换机不建议开启环路检测功能。
- 对以太网接口进行环回测试时，接口将不能正常转发数据包。
- 手工关闭以太网接口时，则不能进行内部环回测试。
- 在进行环回测试时系统将禁止在接口上进行 speed、duplex、mdix-mode 和 shutdown 命令的配置。
- 以太网接口进行环回测试时将工作在全双工状态，环回测试结束后恢复原有配置。
- 目前，我司交换机在 802.1Q 的 VLAN 下的环回测试能实现基本的受控功能；但针对 access、trunk 和 hybird 各个端口的环回测试受控机制处于研发测试中，暂不支持。

2.9 网络诊断

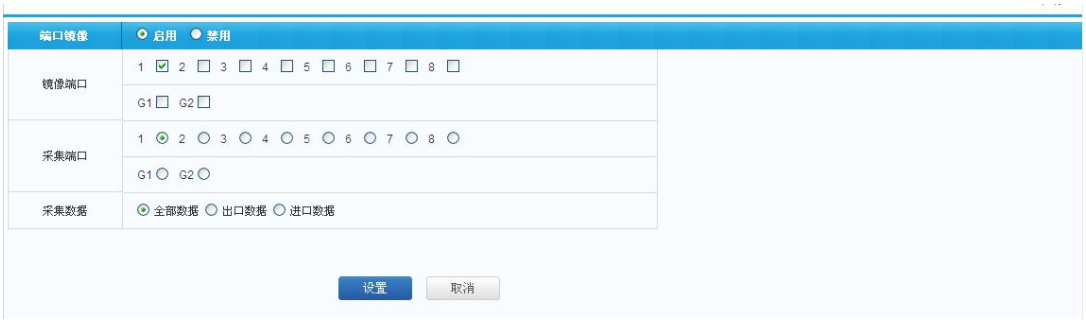
2.9.1 端口镜像

端口镜像就是将被监控端口上的数据复制到指定的监控端口，对数据进行分析和监视。以太网交换机支持多对一的镜像，即将多个端口的报文复制到一个监控端口上。 用户可以指定受监控的报文的方向，如只监控指定端口发送的报文。 采用端口镜像组的方式来配置端口镜像功能。每个端口镜像组包含一个监控端口，和一组被监控端口。

为什么要配置端口镜像？

要想实现针对网络数据进行监控，当然直接可以将 sniffer 工具放置在网络出口处针对所有流出数据包进行监控，不过这样实施最大的问题就是平白无故增加 了一个中间设备，当设备损坏或出现故障后网络传输会中断，从而影响了正常网络访问。即便设备没有问题也会因为增加节点带来速度缓慢的问题，这样也必然影响 整个网络的整体运行效率。

为了解决这种直接拿真正出口作为监控端口的麻烦，网络管理员都采用端口镜像的方法来平白无故创造一个与真实出口一模一样的端口，所有发放到内网各个接口或者 传出端口的数据包都会重复复制后发送到这个镜像端口，这样就可以同时实现不影响网络传输性能的同时对数据流量进行监控了。



镜像端口

该组定义了一组被监控端口，设备将从这些端口采集被指定方向的数据

采集端口

该组定义了一个用于监控端口，设备将从该端口输出被指定方向的数据

采集数据

该参数指定了监视端口数据的方向，一共分"全部"，"进"，"出"三个选择。监视者可以根据自己的选择。

注意：

- 该功能必须在正常使用中被关闭，否则所有基于端口的高级管理功能均无法使用如 RSTP,IGMP SNOOP
- 镜像功能只处理 FCS 正常的包，不能处理各种错误的数据帧

2.9.2 网络诊断

PING (Packet Internet Grope)，因特网包探索器，用于测试网络连接量的程序。Ping 发送一个 ICMP 回声请求消息给目的地并报告是否收到所希望的 ICMP 回声应答。PING 是用来检查网络是否通畅或者网络连接速度的命令。使用 Ping 可以测试计算机名和计算机的 ip 地址,验证与远程计算机的连接,通过将 icmp 回显数据包发送到计算机并侦听回显回复数据包来验证与一台或多台远程计算机的连接

目的主机

指定要 ping 的远程计算机,可以是域名也可以是 IP 地址

报文大小

发送包含数据量长度为"报文长度"的 echo 数据包

报文数目

发送"报文数目"个数指定的 echo 数据包数

报文间隔

指定发送报文的间隔，单位为毫秒

应答超时

指定超时间隔，单位为毫秒

网络诊断

开始发送 Ping 诊断报文

2.10 系统管理

2.10.1 时间配置

NTP 协议全称网络时间协议（Network Time Procotol）。它的目的是在国际互联网上传递统一、标准的时间。具体的实现方案是在网络上指定若干时钟源网站，为用户提供授时服务，并且这些网站间 应该能够相互比对，提高准确度。它可以提供高精准度的时间校正（LAN 上与标准间差小于 1 毫秒，WAN 上几十毫秒），且可介由加密确认的方式来防止恶毒的 协议攻击。

本地时间

使用手动配置的时间来更新设备自身的时间

使用 NTP

使用 NTP 协议的时间来更新设备自身的时间

世界时区

世界时区的划分以本初子午线为标准。从西径 6.5° 到东经 6.5°（经度间隔为 15°）为零地区。由零时区的两个边界分别向东和向西，每隔经度 15° 划一个 时区，东、西各划出 12 个时区，东十二时区与西十二时区相重合；全球共划分成 24 个时区。各时区都以中央经线的地方平太阳时作为本区的标准时。相邻两个时 区的标准时相差一小时。时区界线原则上按照地理经线划分，但在具体实施中往往根据各国的行政区界或自然界线来确定，以方便使用。设备中可以根据典型的地域选择相关的时区，设备根据选择的地区自动调整内部时间的偏移。

自动调整夏令时

夏令时比标准时早一个小时。例如，在夏令时的实施期间，标准时间的上午 10 点就成了夏令时的上午 11 点。夏令时，又称"日光节约时制"或"夏时制"，是一 种为节约能源而人为规定地方时间的制度。目前全世界有近 110 个国家每年要实行夏令时，当选择特定的地域时，如果该地区允许"夏令时"，则该选项可设置，否则灰化无效。

NTP 服务器

可以提供 NTP 定时的主机名或 IP 地址

系统时间

设备自身的时间，上电后按"1970 年 1 月 1 日 0:00:10 星期四"，可手动或自动使用 NTP 更新。

PC 时间

访问者自身 PC 的时间，显示与交换机本身没有关系。

注意：

- NTP 服务器可为空，设备使用自带的服务器更新，但必须 DNS 和网关配置正确
- NTP 服务器不为空，其必须为有效的主机名或合法的 IP 地址
- 只有"管理员"才有权限手动配置设备的时间
- 时区和夏令时必须配置，无论是使用"本地时间"还是"NTP 时间"
- NTP 服务器或者访问者的 PC 的时间配置可以会导致显示不正常，可以改变"时间显示"格式来调整显示

2.10.2 设备地址

DHCP 动态 IP 地址：交换机启用 dhcp-client 功能，获得 IP 地址等参数。

静态 IP 地址：用户手动配置交换机的 IP 地址。

IP 地址

IP 地址是分配给连接在 Internet 上的设备的一个 32 比特长度的地址。IP 地址由两个字段组成：网络号码字段（net-id）和主机号码字段（host-id）。IP 地址由美国国防数据网的网络信息中心（NIC）进行分配。IP 地址采用点分十进制方式记录。每个 IP 地址被表示为以小数点隔开的 4 个十进制整数，每个整数对应一个字节，如 10.110.50.101。

子网掩码

掩码是一个 IP 地址对应的 32 位数字，这些数字中一些为 1，另外一些为 0。原则上这些 1 和 0 可以任意组合，不过一般在设计掩码时，把掩码开始连续的几位设置为 1。掩码可以把 IP 地址分为两个部分：子网地址和主机地址。IP 地址与掩码中为 1 的位对应的部分为子网地址，其他的位则是主机地址。A 类地址对应的掩码为 255.0.0.0；B 类地址的掩码为 255.255.0.0;C 类地址的掩码为 255.255.255.0。 使用掩码把一个可以包括 1600 多万主机的 A 类网络或 6 万多台主机的 B 类网络分割成许多小的网络，每一个小的网络就称之为子网。

默认网关

主机里的默认网关通常被称作默认路由。 默认路由（Default route），是对 IP 数据包中的目的地址找不到存在的其他路由时，路由器所选择的路由。目的地不在路由器的路由表里的所有数据包都会使用默认路由。这条 路由一般会连去另一个路由器，而这个路由器也同样处理数据包：如果知道应该怎么路由这个数据包，则数据包会被转发到已知的路由；否则，数据包会被转发到默认路由，从而到达另一个路由器。

DNS 地址

DNS 的全称是 Domain Name Server，作用是将便于我们记忆的域名，解析成 Internet 可以识别的 IP 地址。如果我们设备需要访问某个主机名，则需要利用这个服务器解析成 IP 地址。

注意：

- 我们可以设置的 IP 地址范围应该为 192.168.x.x, 162.[16-31].x.x, 或 10.x.x.x
- NTP 和 EMAIL 将利用到 DNS 服务，如果应用这两个服务，请务必填写正确的 DNS 地址

2.10.3 系统信息

设备名称

为标示网络中的每个交换机，给每个交换机取一个不同的名称，以便区分，并支持中文输入，交换机名称最长不超过 16 个字节

设备编号

描述交换机安装的位置，支持中文输入，最长不超过 16 个字节

设备描述

对交换机一个概要描述，如此的信息也可以通过一个 SNMP 软件工具搜索到，最长不超过 16 个字节

联系信息

用于技术支持的 Email 或其他联系方式，以便网络出现问题时及时联系

内存使用

- 有效内存：内存总数
- 已用内存：已经使用的内存数
- 空闲内存：空闲的内存数
- 缓冲内存：缓存内存数

CPU 信息

- 微处理器：CPU 的内核家族
- 系统主频：CPU 使用的主频
- 系统特性：CPU 的特征表项

- 系统描述：关于 CPU 的描述

2.10.4 日志信息

- 设备提供日志功能，以供使用者参考可能遇到设置问题。

1、开启日志服务

如果您知道设备的 IP 地址，用户名及密码：

- 使用浏览器登录至网页界面。
- 点击 "系统管理" 标签。
- 点击 "日志信息" 子标签。
- 选择 "日志记录"栏目。
- 点击 "启用" 按钮后保存设置。

2、关闭日志服务

- 如果您知道设备的 IP 地址，用户名及密码：
- 使用浏览器登录至网页界面。
- 点击 "系统管理" 标签。
- 点击 "日志信息" 子标签。
- 选择 "日志记录"栏目。
- 点击 "禁用" 按钮后保存设置。

3、浏览日志

如果您知道设备的 IP 地址，用户名及密码：

- 使用浏览器登录至网页界面。

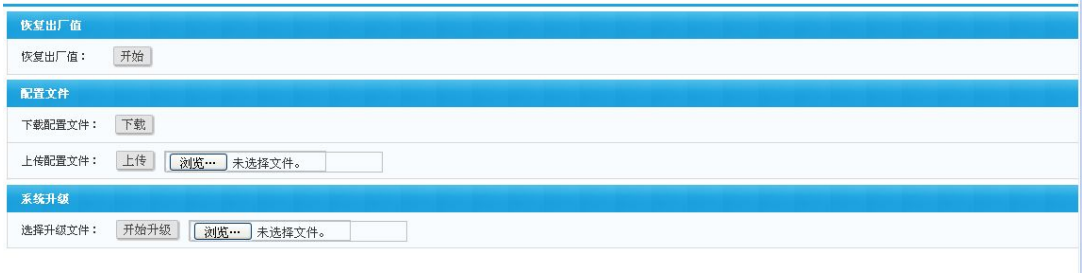
- 点击 "系统管理" 标签。
- 点击 "日志信息" 子标签。
- 选择 "显示类型"栏目。
- 日志列表中按时间顺序显示符合要求的日志

4、删除/下载日志

如果您知道设备的 IP 地址，用户名及密码：

- 使用浏览器登录至网页界面。
- 点击 "系统管理" 标签。
- 点击 "日志信息" 子标签。
- 选择 "信息处理"栏目。
- 点击"清除"将删除所有信息，点击"下载"则下载所有信息

2.10.5 文件管理



1、恢复出厂默认设置

如果您知道设备的 IP 地址，用户名及密码：

- 使用浏览器登录至网页界面。
- 点击 "系统管理" 标签。
- 点击 "文件管理" 子标签。
- 选择 "恢复出厂值"栏目。
- 点击 "开始" 按钮。
- 提示"以后 IP 地址将恢复为'192.168.1.253'"，确认后开始恢复出厂值设置。
- 将开启一个新页面，输入 "192.168.1.253"将进行新的配置。

2、下载配置文件

如果您知道设备的 IP 地址，用户名及密码：

- 使用浏览器登录至网页界面。
- 点击 "系统管理" 标签。
- 点击 "文件管理" 子标签。
- 选择 "下载配置文件"栏目。
- 点击 "下载" 按钮。
- 选择文件保存的目录和名字。

3、上传配置文件

如果您知道设备的 IP 地址，用户名及密码：

- 使用浏览器登录至网页界面。
- 点击 "系统管理" 标签。
- 点击 "文件管理" 子标签。
- 选择 "上传配置文件"栏目。
- 点击 "浏览" 按钮，选择要上载文件的位置。
- 点击 "上传" 按钮。
- 更新完成后将自动开启一个新页面到"系统状态"。

4、系统升级

如果您知道设备的 IP 地址，用户名及密码：

- 使用浏览器登录至网页界面。
- 点击 "系统管理" 标签。
- 点击 "文件管理" 子标签。
- 选择 "选择升级文件"栏目。
- 点击 "浏览" 按钮，选择要上载文件的位置。
- 点击 "开始升级" 按钮。
- 提示"升级过程中禁止断电"，确认后开始烧写 flash。
- 升级完成后将自动开启一个新页面到"系统状态"。

注意：

- 恢复出厂值设置将导致设置的所有状态处于刚出厂的状态，其设置的 IP 是静态 IP 地址"192.168.1.253"。
- 升级中断电请立即将产品邮寄到销售公司以寻求可能的解决办法。

上海总部：

电 话：021-67756421/2/3/4/5/6/9

服务热线：400-66-12508

传 真：021-67756427

邮 编：201615

邮 箱：mexontec@mexontec.com

地 址：上海市松江高科技园区九泾路 959 号豪禹创业园北座 6F、4F

南京办事处:电话：025-66916358

成都办事处:电话：028-87606176

北京办事处:电话：010-62931243

深圳办事处:电话：0755-26403312

西安办事处:电话：029-88223137