

MOXA 以太网交换机

EDS-726 系列用户手册

www.moxa.com/product

2006 年 8 月（第一版）

MOXA®

Moxa Networking Co., Ltd.

电话: +886-2-2910-1230

传真: +886-2-2910-1231

网址: www.moxa.com

MOXA 技术支持

全球: support@moxanet.com

美国: support@usa.moxa.com

MOXA 以太网交换机 EDS-726 系列用户手册

在使用本手册之前，请您认真阅读以下使用许可协议。只有在同意以下使用许可协议的情况下方能使用本手册中介绍的产品。

版权公告

Copyright © 2006 Moxa Networking Co., Ltd. All rights reserved.
未经 MOXA 公司书面允许任何公司或个人不得以任何形式复制本手册全部或部分內容。

商标

MOXA 是 MOXA 公司的注册商标，本手册中的其他商标分别属于各自的公司所有。

重要声名

MOXA 公司在本手册中提供的任何信息，并不代表对这些信息提供了相应的授权。

MOXA 公司努力使本手册中提供的信息准确和适用，然而 MOXA 并不对这些信息的使用承担任何责任，也不对这些信息的使用承担任何连带责任。

产品及使用手册可能包含技术或印刷上的错误。MOXA 公司保留在不事先通知情况下更改本使用手册全部或部分内容的权力。

目录

第 1 章	简介.....	1-1
	概述.....	1-2
	产品包装核对表.....	1-2
	产品特点.....	1-2
	高效能工业网络交换技术.....	1-2
	针对工业应用的设计.....	1-2
	有用组件和远程配置.....	1-3
	推荐使用的软件和附件.....	1-3
第 2 章	开始.....	2-1
	RS-232 串口控制台(115200, None, 8, 1, VT100).....	2-2
	Telnet 远程控制台配置.....	2-5
	Web 浏览器配置.....	2-6
	禁用 Telnet 和浏览器.....	2-8
第 3 章	功能特性.....	3-1
	概述.....	3-2
	配置基本设置.....	3-2
	系统识别.....	3-2
	密码.....	3-3
	允许访问 IP 地址.....	3-4
	端口.....	3-5
	网络.....	3-7
	时间.....	3-8
	系统文件升级—通过远程 TFTP.....	3-10
	系统文件升级—通过本地导入/导出.....	3-11
	系统文件升级—通过 CF 卡.....	3-11
	出厂设置.....	3-12
	使用链路聚合.....	3-12
	链路聚合的概念.....	3-13
	配置链路聚合.....	3-14
	配置 SNMP.....	3-15
	SNMP 读/写设置.....	3-16
	Trap 设置.....	3-18
	Private MIB 信息.....	3-18
	通信冗余功能.....	3-18
	千兆冗余以太网环网自愈能力 (< 300 ms).....	3-19
	Turbo Ring 的概念.....	3-19
	设置 Turbo Ring.....	3-22
	STP/RSTP 的概念.....	3-23
	设置 STP/RSTP.....	3-28
	流量优先级功能.....	3-30
	流量优先级的概念.....	3-30
	配置流量优先级.....	3-32
	VLAN 功能.....	3-35
	VLAN 的概念.....	3-35
	MOXA EDS-726 VLAN 功能的应用.....	3-37

	配置 802.1Q VLAN	3-38
	Multicast过滤功能	3-39
	Multicast过滤的概念	3-40
	配置IGMP Snooping	3-43
	加入静态multicast MAC	3-45
	配置GMRP	3-46
	带宽管理	3-47
	配置带宽管理	3-47
	使用端口访问控制	3-48
	配置IEEE 802.1X	3-50
	静态端口锁定	3-53
	自动报警功能	3-54
	配置E-mail报警	3-54
	E-mail报警事件设置	3-54
	Email设置	3-56
	配置继电器报警	3-57
	继电器报警事件设置	3-57
	继电器报警列表	3-58
	Line-Swap-Fast-Recovery功能	3-59
	配置Line-Swap Fast Recovery	3-59
	Set Device IP功能	3-59
	配置Set Device IP	3-60
	诊断功能	3-61
	镜像端口	3-61
	Ping	3-62
	监视器功能	3-62
	交换机监视	3-62
	端口监视	3-63
	MAC地址表功能	3-63
	事件日志功能	3-64
第 4 章	EDS配置器图形用户界面	4-1
	启动EDS配置器	4-2
	广播搜索	4-2
	通过IP地址搜索	4-3
	升级固件	4-4
	修改IP地址	4-5
	导出配置文件	4-5
	导入配置文件	4-6
	解除服务器的锁定	4-7
附录 A	MIB组	A-1
附录 B	规格	B-1
附录 C	服务信息	C-1
	MOXA Internet服务	C-2
	故障报告单	C-3
	返修流程	C-4

1

简介

欢迎使用 MOXA EDS-726 系列产品，该模组化的千兆以太网交换机专为应用于工业领域的以太网设备联网而设计。

本章包括以下内容：

- 概述
- 产品包装核对表
- 产品特点

概述

EDS-726 的出现让网络规划变得更加容易且灵活。模组化的设计方便您在一台交换机上可以安装 2 个千兆网口和 24 个快速以太网口。您可以从 5 种一口的千兆模块（RJ45 接口或光纤接头）和 8 种四口的快速以太网模块（RJ45 接口或 SC/ST 光纤接头）中选择。EDS-726 适合任何工业上的应用，同时也方便系统将来升级。产品特点包括人性化的 LED 灯显示角度（便于工程师观察），插入式 CF 卡用于备份配置信息，网络冗余功能以及智能化的网络管理。该产品具备相当高的灵活性、可靠性以及导向式的应用功能，完全可以满足任何苛刻工业环境的应用。

产品包装核对表

MOXA EDS-726 随机附带以下物品。若有遗失或损坏，请联系客户服务工程师以便取得帮助。

- 1 MOXA EDS-726 模块化交换机或相应的模块
- 硬件安装使用手册
- 包含用户使用手册和用于 EDS-726 模块化交换机系统的 Windows Utility 的光盘
- MOXA 产品授权手册
- 专用于 EDS-726 模块化交换机系统的 RS-232 端口线(RJ45 到 DB9)

注意：以上物品如有任何遗失或损坏，请联系 MOXA 销售代表或客户服务工程师以便取得帮助。

产品特点

高效能工业网络交换技术

- 冗余自愈千兆以太环网（全负载下恢复时间 < 300 ms）
- 用于过滤工业以太网协议中 multicast 流量的 IGMP Snooping 和 GMRP
- 支持 IEEE802.1Q VLAN 和 GVRP 协议方便网络规划
- 支持 QoS—IEEE802.1p/1Q 和 TOS/DiffServ 增加决定权
- 支持 802.3ad, LACP 有利于带宽优化
- 支持 IEEE 802.1X 和 SSL 提高网络安全性
- SNMP V1/V2c/V3 使得不同层次的网络管理均具有安全性

针对工业应用的设计

- 模块化管理的交换机，最多扩张至 26 个端口。可从以下模块中选择：
 - 5 种一口千兆模块，10/100/1000BaseT(X)（RJ45 接头）或 1000BaseSX/LX（SC 接头）
 - 8 种四口快速以太网模块，具备 10/100BaseT(X)（RJ45 接头）和 100BaseFX（单模/多模，SC/ST 接头）
- 用于升级固件和加载/保存配置的 CF 卡
- 远程传输距离可达 40km 或 80km
- 冗余的双直流电源输入
- IP30，波浪型的高强度外壳设计
- 导轨或面板安装

- 带宽管理功能可以防止不可预料的网络状况
- 端口锁定只允许授权的 MAC 地址访问
- 端口镜像可用于在线调试功能
- 意外发生时通过 E-mail，继电器输出自动报警
- DI 接口可完成传感器、报警器与 IP 网络的整合
- 自动恢复连接设备的 IP 地址
- Line-swap 快速恢复

有用组件和远程配置

- 通过使用 Web 浏览器，Telnet/RS-232 串口控制台，Windows Utility 进行配置
- 可发送 Ping 指令判断网络的完整性

推荐的软件和附件

- EDS-SNMP OPC Server Pro
- DR-4524, DR-75-24, DR-120-24 24 VDC 导轨电源
- WK-32: 壁挂安装套件

2

开始

本章将介绍第一次如何访问 EDS-726。访问该交换机有三种方法：串口控制台，Telnet 控制台和 Web 浏览器。串口控制台连接方法就是用串口线将 EDS-726 连接到 PC 机的 COM 口，可以在不知道 EDS-726 的 IP 地址的情况下使用。而 Telnet 和 Web 浏览器方式则用于通过局域网或 Internet 访问 EDS-726。

包括以下内容：

- RS-232 串口控制台(115200, None, 8, 1, VT100)**
- Telnet 远程控制台配置**
- Web 浏览器配置**
- 禁用 Telnet 和浏览器**

RS-232 串口控制台(115200, None, 8, 1, VT100)

注意:

连接警告!

1. 不能同时使用串口控制和 Telnet 连接 EDS-726。
2. 可以同时使用 Web 浏览器和串口控制台连接 EDS-726, 或者也可以同时使用 Web 浏览器和 Telnet 连接 EDS-726。
尽管如此, 我们还是建议您不要同时使用两种以上的连接方式。这样可以让您更加方便有效地来配置 EDS-726。

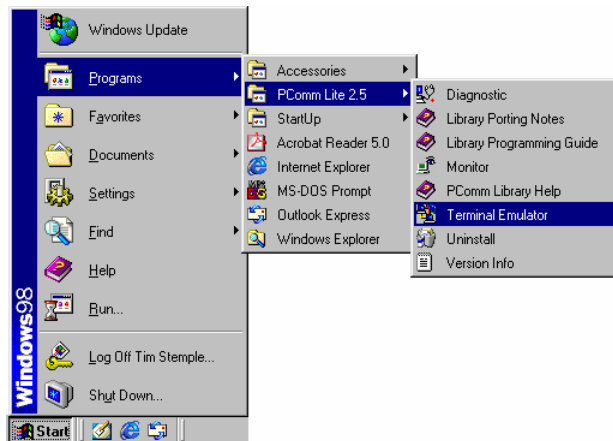
注意:

我们建议您使用 MOXA PComm Terminal Emulator 软件, 您可以在 Moxa 网站上免费下载。

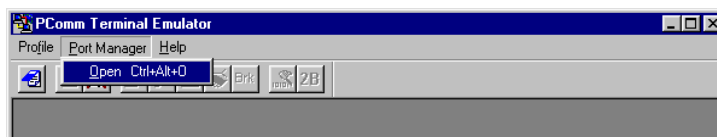
在运行 PComm Terminal Emulator 之前, 请使用 RJ45 转 DB9-F (或 RJ45 转 DB25-F) 电缆连接 EDS-726 的 RS-232Console 口和 PC 机的 COM 口(取决于您 PC 机的设置, 通常是 COM1 或 COM2)。

PComm Terminal Emulator 安装完毕之后, 按照以下步骤进入 RS-232Cosole。

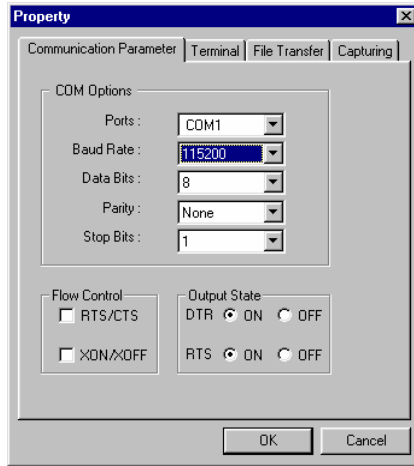
1. 在 WINDOWS 桌面, 点击 **开始** → **程序** → **PCommLite2.5** → **Terminal Emulator**。



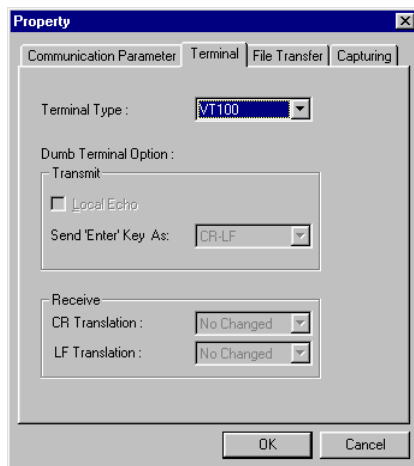
2. 在 **Port Manager** 下选择 **Open** 打开一个新的连接。



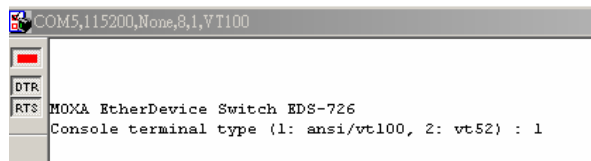
3. 在 Property 窗口打开后选择 **Communication Parameter** 给控制台连接选择合适的 COM 口，波特率为 115200，8 为数据位，无校验，1 为停止位。



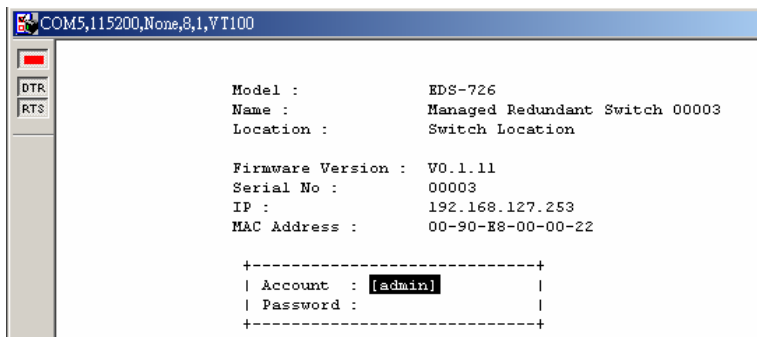
4. 点击 **Terminal**，在 **Terminal Type** 上选择 **VT100**。点击 **OK** 继续。



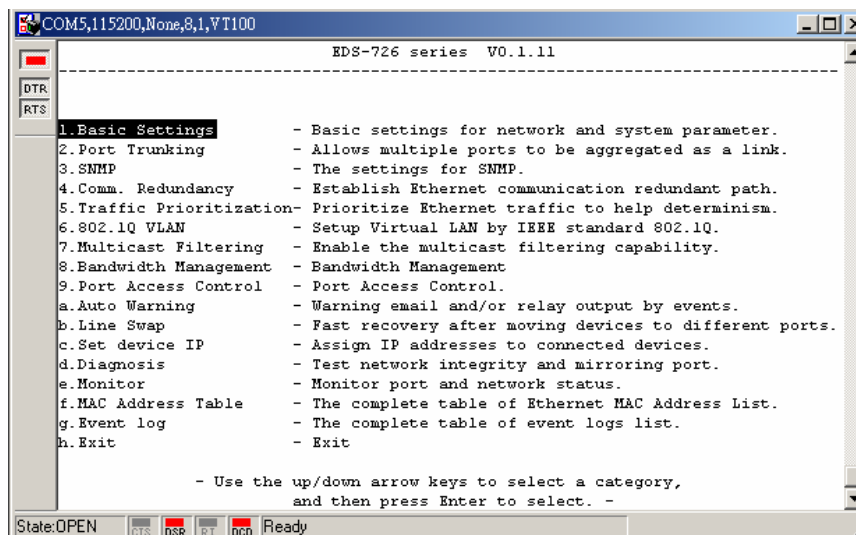
5. 输入 1 来将 Terminal Type 设为 **ansi/VT100**，然后按回车。



6. 屏幕上会出现 **Console** 登陆画面。按 **Enter** 打开帐户选择器，选择 **admin** 或 **user**。在键盘上使用向下键将光标移到密码区，输入 **Console** 密码（该密码同 **Web** 服务器一样；如果没有设置过 **console** 密码，让其为空即可），然后按 **Enter** 键。



7. 此时将出现 EDS-726 的主菜单。（注意：如果想改变 **PComm Terminal Emulator** 窗口的外观，请选择 **Menu** 菜单下的 **Font...** 然后选择相应的格式选项。）



8. 进入主菜单之后，使用以下键来移动光标并更改选项。

按键	功能
Up/Down/Left/Right arrows, or Tab	移动光标
Enter（回车）	显示，选项选择
Space（空格）	选项切换
Esc	上层菜单

Telnet 远程控制台配置

您可以使用 Telnet 登陆在网络中访问 EDS-726 的 Console 端口。为了能够通过和 EDS 连接在相同局域网中的 PC 主机通过网络（远程控制台或 Web 浏览器）访问 EDS 的各项功能，我们必须确保 PC 主机和 EDS 属于同一个逻辑子网。检查您的 PC 主机的 IP 地址和掩码，一般默认的 EDS-726 的 IP 地址是 192.168.127.253，掩码为 255.255.0.0 (B 级网络)。如果不改变这些值，那么您的 PC 主机的掩码就是 255.255.0.0，而 IP 地址必须是 192.168.xxx.xxx 的形式。换个角度来说，如果 PC 主机的子网掩码为 255.255.255.0，那么 IP 地址必须是 192.168.127.xxx 的形式。

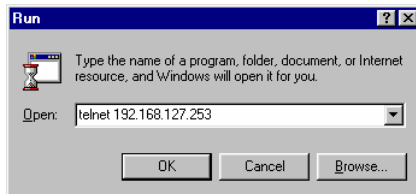
注意： 利用和 EDS-726 连接在相同局域网中的 PC 主机通过网络访问 EDS-726 的管理和监控功能时，必须确保 PC 主机和 EDS-726 属于同一个逻辑子网。

注意： 在通过 Telnet 访问控制台端口之前，先把 EDS-726 的 RJ45 连接到以太网当中，或者直接连接到 PC 主机的以太网卡，通过直连线和交叉线均可。

注意： EDS-726 的默认 IP 是 192.168.127.253。

按照以下步骤通过 Telnet 访问 Console 端口：

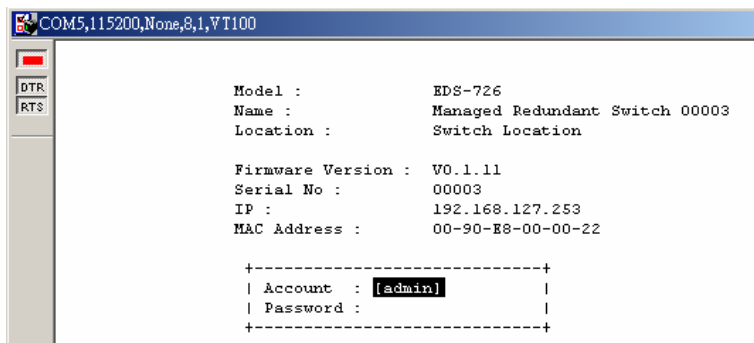
1. 点击开始—运行，在 Windows 的运行窗口中输入要 Telnet 的 EDS-726 的 IP 地址。（或从 MS-DOS 提示命令中输入 Telnet 命令。）



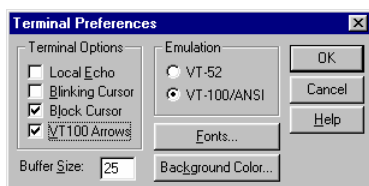
2. 输入 1 选择 **ansi/VT100**，按回车。

```
MOXA EtherDevice Switch EDS-726
Console terminal type (1: ansi/vt100, 2: vt52) : 1
```

3. 屏幕上会出现 Console 登陆画面。按 Enter 打开帐户选择器，选择 admin 或 user。在键盘上使用向下键将光标移到密码区，输入 Console 密码（该密码同 Web 服务器一样；如果没有设置过 console 密码，让其为空即可），然后按 Enter 键。



4. 此时将出现 EDS-726 的主菜单，在窗口顶部的菜单中点击 Terminal 菜单下选择 Preference。
5. 在 Terminal Preferences 窗口中，确认 VT100 Arrows 选项已被选定。



注意： Telnet Console 的界面和操作与 RS-232 Console 非常相似。

Web 浏览器配置

MOXA EDS-726 以太网交换机的 Web 浏览器接口为修改交换机设置和访问内建的监视和网络管理功能提供了一种简便的方法。您可以使用 Internet 浏览器或 Netscape 浏览器来访问 EDS-726。

注意： 和 EDS-726 连接在相同局域网中的 PC 主机要使用 EDS-726 的管理和监控功能，必须确保 PC 主机和 EDS-726 属于同一个逻辑子网。

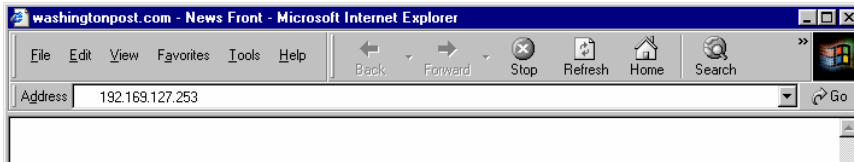
注意： 如果 EDS-726 是按照别的 VLAN 来设置的，必须确定您的 PC 主机能够对 VLAN 进行管理。详情请参考第三章的 802.1Q VLAN 设置。

注意： 在访问 EDS-726 Web 浏览器之前，先把交换机的 RJ45 端口连接到局域网或 PC 主机的以太网卡，通过交叉线或直连线均可。

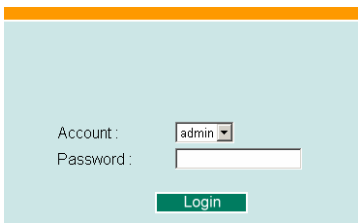
注意： MOXA EDS-726 的默认 IP 地址是 192.168.127.253。

按照以下步骤访问交换机的 Web 浏览器：

1. 打开 Internet 浏览器，输入 EDS-726 的 IP 地址，然后按回车键建立一条连接。

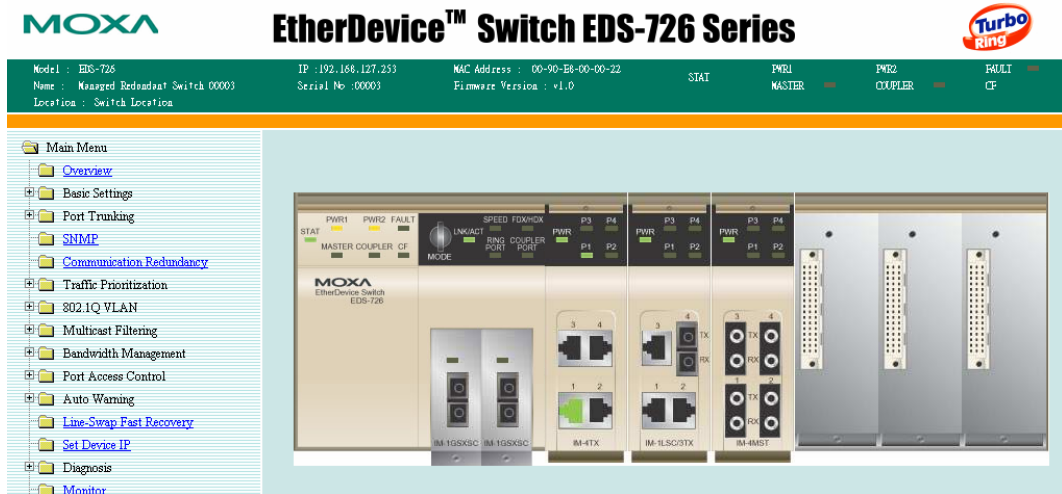


2. 登陆页面打开后，选择登陆帐号（Admin 或 User）并键入密码（与 Console 密码一致），点击 Login 继续。若未设置过密码，则保持密码区未空即可。



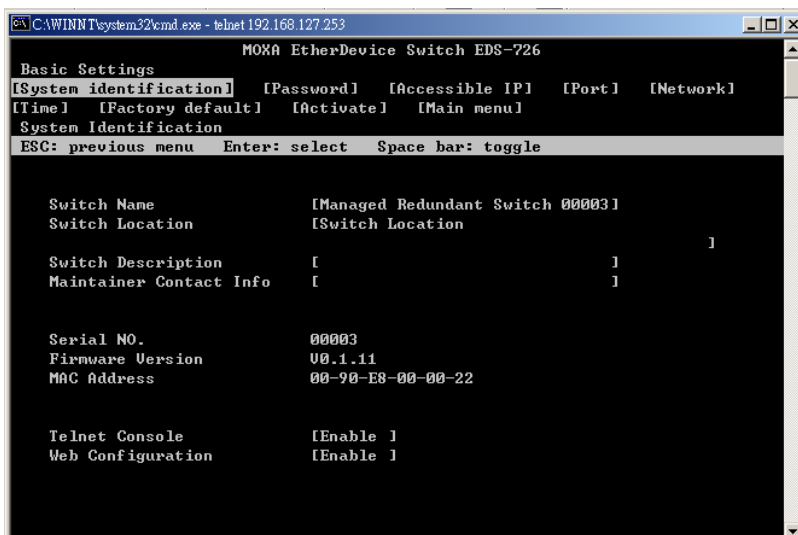
注意： 默认情况下，EDS-726 的密码未设置，为空。

您需要等待一会，将网页下载到您的计算机。使用左边的菜单树打开功能页面来访问 MOXA EtherDevice Switch 的各项功能。



禁用 Telnet 和浏览器

如果您将 EDS-726 连到了公网中, 而又不想通过网络使用其管理功能, 我们建议您从 RS-232 Console 的 Basic Setting → System Identification 页面当中将 Telnet Cosole 和 Web Configuration 功能禁掉, 如下图所示。



本章介绍如何访问 EDS-726 的各种配置, 监控和管理功能。访问这些功能有三种方式: RS-232 串口控制台, 远程控制台和 Web 浏览器。串口控制台连接方法就是用串口线将 EDS-726 连接到 PC 机的 COM 口, 可以在不知道其 IP 地址的情况下使用。而远程控制台和 Web 浏览器方式可用于在局域网或 Internet 中访问 EDS-726。

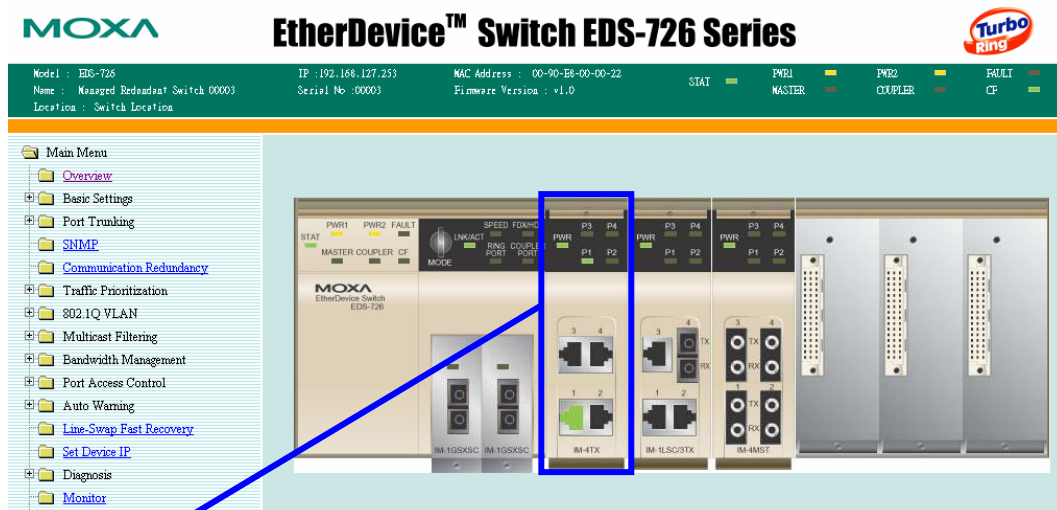
Web 控制台是配置 EDS-726 最容易的方式。本章用 Web 控制台来介绍这些功能。Web Console、Telnet Console 以及串口 Console 之间并没有太大的区别。

包括以下内容:

- 概述
- 配置基本设置
- 使用端口聚合
- 配置 SNMP
- 通信冗余功能
- 流量优先级功能
- VLAN 功能
- Multicast 过滤功能
- 带宽管理
- 使用端口访问控制
- 自动报警功能
- Line-swap-Fast-Recovery 功能
- Set Device IP 功能
- 诊断功能
- 监视器功能
- MAC 地址表功能
- 事件日志功能

概述

在 Overview 页面上实时显示了您所安装的 EDS-726 正面视图。该视图如您站在 EDS-726 前方所看到的界面一样。将鼠标移到交换机上并点击鼠标左键便可以观察到模块上 LED 灯的不同状态。通过该图，您可以查看并更改网络上 EDS-726 的状态。



激活端口显示为绿色，未激活的端口显示为黑色。

需要注意的是，图中所示的模块名称应与交换机上使用的模块匹配。

配置基本设置

基本设置组包括管理员维护控制 EDS-726 要经常使用的一些设置。

系统识别

系统识别显示在网页的最上端，将包括在报警 email 中。设置好系统识别项将有助于更加方便地识别出连接到网络上的不同交换机。

Switch Name

设置	说明	出厂设置
不超过 30 个字符	用于指定不同 EDS-726 的功用。如工厂交换机 1	Industrial Redundant Switch[序列号]

Switch Location

设置	说明	出厂设置
不超过 80 个字符	指明不同 EDS-726 的位置，如生产线 1	Switch Location

Switch Description

设置	说明	出厂设置
不超过 30 个字符	关于不同交换机的详细信息	无

Maintainer Contact Info

设置	说明	出厂设置
不超过 30 个字符	设备维护人员的联系方式。	无

密码

EDS-726 提供了两种权限供用户访问：管理员（admin）权限允许用户访问且可修改所有 EDS-726 的所有配置参数，而用户（user）权限仅供用户查看设置，不能更改。

**注意**

EDS-726 的默认密码为空。如果已经设定好密码，通过 RS-232Console、Telnet Console 或 Web 浏览器访问交换机时必须输入密码。

Account

設置	说明	出厂设置
admin	“admin”权限允许更改所有 EDS-726 设置	admin
user	“user”权限只能查看 EDS-726 设置	

Password

設置	说明	出厂设置
旧密码 (不超过 16 个字符)	更改密码时先输入当前密码	无
新密码 (不超过 16 个字符)	输入新密码	无
重输新密码 (不超过 16 个字符)	再输一次新密码	无

Password Setting

Account Name :

Old Password :

Type Old Password :

New Password :

Retype Password :

允许访问 IP 地址

MOXA EDS-726 是利用基于 IP 地址过滤的方法来控制对其的访问。

Accessible IP List

Enable the accessible IP list ("Disable" will allow all IP's connection)

Index	IP	NetMask
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

允许访问 IP 设置可以让你添加或删除合法的远程主机 IP 地址，从而阻止未经授权的访问。这就意味着，如果一个主机 IP 地址存在于允许访问 IP 地址表中，那这台主机就能访问 EDS-726。通过设置参数，你可以做到以下任意一点。

- **只有指定 IP 地址的主机能访问 EDS-726**
输入 IP 地址/255.255.255.255 (例如 192.168.1.1/255.255.255.255.)
- **指定子网中的主机能访问 EDS-726**
输入 IP 地址/255.255.255.0 (例如 192.168.1.0/255.255.255.0.)
- **任何主机能访问 EDS-726**
通过选择 “Enable the accessible IP list”来禁用该功能。

更多设置示例如下表所示：

允许主机	格式
任何主机	禁用
192.168.1.120	192.168.1.120 / 255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0 / 255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0 / 255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0 / 255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128 / 255.255.255.128

端口

端口设置可以让用户控制端口访问、端口传输速率、流量控制以及端口类型。具体每项设置如下。

Port	Enable	Description	Name	Speed	FDX Flow Ctrl	MDI/MDIX
2-1	<input checked="" type="checkbox"/>	100BaseTX, RJ45.		Auto	Enable	Auto
2-2	<input checked="" type="checkbox"/>	100BaseTX, RJ45.		Auto	Enable	Auto
2-3	<input checked="" type="checkbox"/>	100BaseTX, RJ45.		Auto	Enable	Auto
2-4	<input checked="" type="checkbox"/>	100BaseTX, RJ45.		Auto	Enable	Auto

Activate

Enable

设置	说明	出厂设置
选择	允许通过端口传输数据	禁止所有端口
未选择	立即禁止访问该端口	

**注意**

如果网络的部分设备或子网瘫痪，管理员可以通过 Advanced Settings/Port 下的 Disable 选项立即禁止访问此端口。

Description

設置	说明	出厂设置
传输介质类型	记录各模块端口所接的传输介质类型	无

Name

設置	说明	出厂设置
不超过 63 个字符	为每个端口指定一个别名，方便管理员记住重要的端口。例如 PLC1	无

Port Transmission Speed

設置	说明	出厂设置
Auto	允许端口和连接设备按照 IEEE 802.3u 自动调节速率	自动调节
100M-Full	如果所连接的设备无法自动协调线性速率，从中选择一项来确定其通信速率。	
100M-Half		
10M-Full		
10M-Half		

FDX Flow Control

当端口传输速率设置为自动调节模式时，该选项可以启用或禁用该端口的流量控制功能。最终取决于 EDS-726 以及其连接的设备之间的自动调节过程。

設置	说明	出厂设置
启用	在自动调节模式下启用流量控制功能	禁用
禁用	在自动调节模式下禁用流量控制功能	

Port Type

設置	说明	出厂设置
Auto	端口可以自动检测相对应的设备的端口类型，再对自身端口类型做相应更改	自动
MDI	如果对应设备不能自动调整端口类型，选择以上两种端口类型之一。	
MDIX		

网络

网络配置功能允许用户修改常规的 TCP/IP 网络参数。详细配置信息如下：

Network Parameters
General Settings

Auto IP Configuration: Disable

Switch IP Address: 192.168.127.253

Switch Subnet Mask: 255.255.255.0

Default Gateway:

1st DNS Server IP Address:

2nd DNS Server IP Address:

Activate

Auto IP Configuration

設置	说明	出厂设置
Disable	手动设置 EDS-726 的 IP 地址	Disable
By DHCP	通过网络 DHCP 服务器自动设置 EDS-726 的 IP 地址	
By BootP	通过网络 BootP 服务器自动设置 EDS-726 的 IP 地址	

Switch IP Address

設置	说明	出厂设置
IP Address of EDS-726	识别 TCP/IP 网络中的 EDS-726	192.168.127.253

Switch Subnet Mask

設置	说明	出厂设置
Subnet mask of the EDS-726	识别 EDS-726 所连接网络的类型 如果是 B 类网络，输入 255.255.0.0，C 类网络输入 255.255.255.0	255.255.255.0

Default Gateway

設置	说明	出厂设置
Default Gateway of the EDS-726	如果您的 LAN 连接到外部网络。输入路由器的 IP 地址	无

DNS IP Address

設置	说明	出厂设置
1 st DNS Server's IP Address	输入当前网络首选 DNS 服务器的 IP 地址。输入完成后，您可以在浏览器的地址栏中输入 EDS-726 的网址（如 www.eds.company.com ），而不需要直接输入 IP 地址	无
2 nd DNS Server's IP Address	输入当前网络备用 DNS 服务器的 IP 地址。当 EDS-726 无法连接首选 DNS 服务器时，会尝试和备用 DNS 服务器连接	无

时间

EDS-726 能够根据 NTP 服务器或者用户指定的时钟校对信息校对时钟。诸如自动 Email 报警功能就可以将实时信息添加到其信息当中。

注意：

EDS-726 没有实时时钟。用户必须在每次重启 EDS-726 之后更新 Current Time 和 Current Date，设置当前时间，尤其是当无法连接 Internet 上的 NTP 服务器或 LAN 上没有 NTP 服务器时。

Current Time

設置	说明	出厂设置
User adjustable time	该参数可以让用户设定本地 24 小时格式的时间	00h:00m:00s

Current Date

設置	说明	出厂设置
User adjustable date	该参数供用户设定本地 yyyy-mm-dd 格式的日期	1970/01/01

System Up Time

显示系统从冷启动开始上电的时间。单位为秒。

Time Zone

設置	说明	出厂设置
User selectable time zone	时区设置可以将 GMT 转换为当地时间	GMT (Greenwich Mean Time)

注意： 时区的更改将自动调整当前时间。请务必在设置时间之前调整时区。

Time Server IP/Name

設置	说明	出厂设置
1 st Time Server IP/Name	IP 地址或域名 IP/Name (如 192.168.1.1 或 time.stdtime.gov.tw/ time.nist.gov)	无
2 nd Time Server IP/Name	当 EDS-726 无法连接首选 NTP 服务器时, 会尝试和备用 NTP 服务器连接	

Time Server Query Period

設置	说明	出厂设置
Query Period	该参数决定从 NTP 服务器上更新时间的频率	600s

系统文件升级—通过远程 TFTP

MOXA EDS-726 支持将系统文件保存到远程 TFTP 服务器或本地主机上，以供别的 EDS-726 以后使用相同的设置，也可以保存日志文件供以后参考。另外也支持从 TFTP 服务器或本地主机上下载预先保存好的固件和设置文件，从而可以很方便的对 EDS-726 升级或更新设置。

TFTP Server IP/Name

設置	说明	出厂设置
IP Address of TFTP Server	远程 TFTP 服务器的 IP 地址或名称，必须在下载或上传文件前设置	无

Configuration Files Path and Name

設置	说明	出厂设置
不超过四十个字符	在 TFTP 服务器上 EDS-726 配置文件的路径和文件名	无

Firmware Files Path and Name

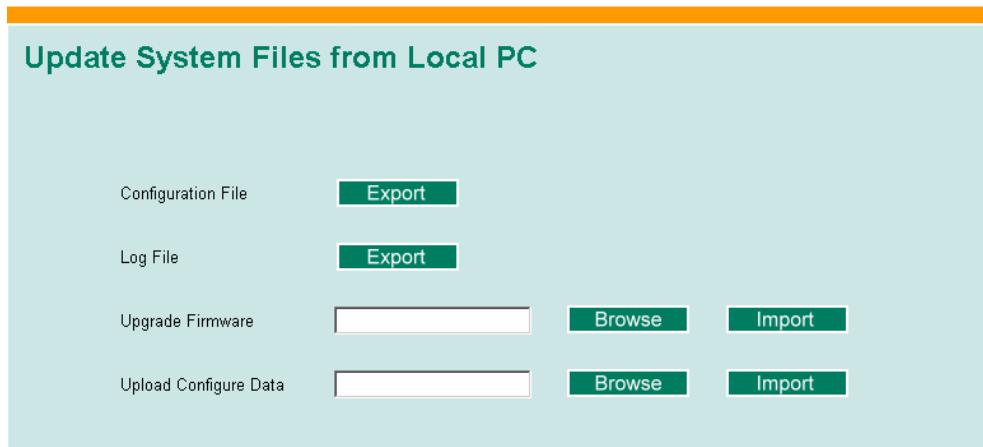
設置	说明	出厂设置
不超过四十个字符	EDS-726 的 firmware 文件路径和文件名称	无

Log Files Path and Name

設置	说明	出厂设置
不超过四十个字符	EDS-726 日志文件的路径和文件名	无

设置好路径和文件名之后，点击 Active 来保存这些设置，随后再按 Download 将存放于远程 TFTP 服务器上的文件下载到 EDS-726，或按 Upload 将要上载的文件上传到远程 TFTP 服务器上。

系统文件升级—通过本地导入/导出

**Configuration File**

点击 Export 可以将 EDS-726 的配置文件导出至本地主机。

Log File

点击 Export 可以将 EDS-726 的日志文件导出至本地主机。

注意： 一些操作系统会直接从 web 网页中打开配置文件和日志文件。这种情况下，请右键单击“Export”按钮保存文件。

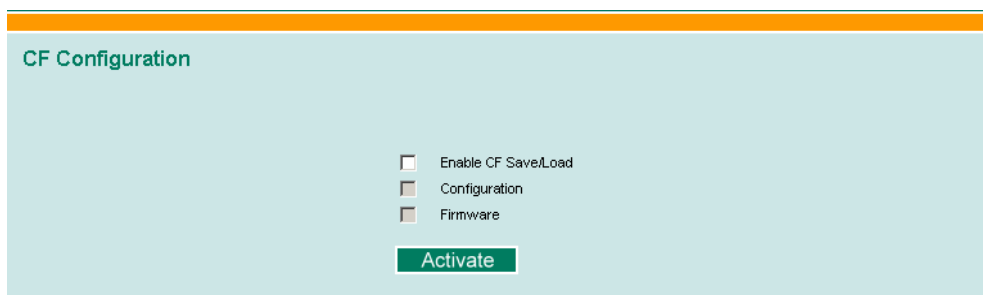
Upgrade Firmware

通过点击 Browse，可以选择您的计算机上保存的 firmware 文件，然后将正确的 firmware 文件导入 EDS-726。当您点击 Import 之后，该升级过程将自动执行。

Upload configure Data

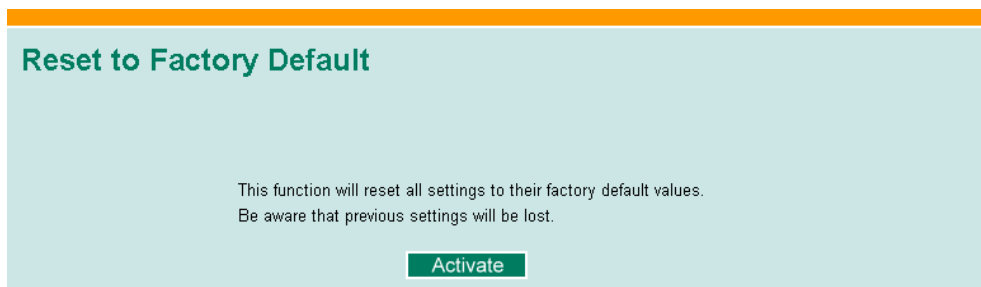
通过点击 Browse，可以选择您的计算机上保存的配置文件，然后将正确的配置文件导入 EDS-726。当您点击 Import 之后，该升级过程将自动执行。

系统文件升级—通过 CF 卡



設置	说明	出厂设置
Enable CF Save/Load	启用从 CF 卡保存和加载配置或 firmware 功能	未选择
Configuration	选择启用从 CF 卡保存和加载配置文件（在启用 CF Save/Load 功能时自动选择该功能）	无
Firmware	选择启用从 CF 卡保存和加载 firmware	无

出厂设置



Factory Default 功能为用户提供了一种简捷的方式来恢复 EDS-726 的出厂默认设置。该功能可以通过 Console（串口或 Telnet）和 Web 浏览器来访问。

注意： 在激活出厂设置功能后，您需要利用默认网络设置重新建立和 EDS-726 的 Web 浏览器或远程连接。

使用链路聚合

链路聚合技术将多条物理链路当作一条单一的聚合逻辑链路使用，MAC Client 可以将该链路视为一个独立的链路。

EDS-726 的链路聚合功能可以通过聚合链路实现四路设备并行通信，其中每路连接最多有 8 个端口。如果其中一个端口通讯失败，其他七个端口作为备援并自动分担网络上的流量。

借助该功能，可以在两台 EDS-726 之间聚合 8 个端口。如果两台交换机上的所有端口均被配置为 100BASE-TX，全双工形式，则此连接的带宽便为 1.6 Gbps。



链路聚合的概念

EDS-726 最多支持 4 个链路聚合组，每个链路聚合组可以实现 8 条链路聚合。您可以将链路聚合组配置为“Static”或“LACP”。将链路聚合组设置为“LACP”时，该组当中的所有端口将启用 LACP。而位于“Static”链路聚合组的端口以及其他非链路聚合组所属的端口都将禁用 LACP。被设置为 LACP 的端口将同组内其他端口交换 LACPDU，以此完成数据传输任务。如果组内所有端口出现了阻塞、禁用或连接失败的情况，那么链路聚合组的功能将失效，同时用户可以观察到该组 LACP 失效的信息。

在一个链路聚合组中，EDS-726 允许用户设置的端口数目可以大于 8 个。超出正常设置范围的端口将依照 IEEE 802.3ad 协议被设置为备用端口。备用端口从属于链路聚合组，具有 LACP 的功能，但没有被激活，其状态显示为阻塞。备用链路聚合组不能被任一链路组采用，也不可以单独作为一条链路被激活。若组内任一端口由于硬件损坏而导致无法通信时，同组的备用端口将会立即取代该损坏端口的工作。在任一 LACP 链路聚合组当中，EDS-726 允许最多有 4 个备用端口。这就意味着各 LACP 链路聚合组最多可以配备 12 个端口。而 Static 链路聚合组不支持备用端口，每组最多可以配备 8 个端口。

链路聚合通常应用在一些骨干联网设备和存在流量瓶颈的网络当中。它具有以下优点：

- 由于链路带宽可以增加至原有带宽的 8 倍，因此可以让客户更加灵活地设置网络。
- 具备冗余功能——在任何一条链路通信失败的情况下，其余链路会自动分担网络上的流量。EDS-726 允许每个 LACP 链路聚合组最多配置 4 个备用端口，换句话说，就是每个 LACP 链路聚合组最多可以配置 12 个端口。这 4 个备用端口为 8 个链路聚合端口提供备份，若组内任一端口由于硬件损坏而导致无法通信时，同组的备用端口将会立即取代该损坏端口的工作。
- 平衡负载——多条链路共同分担 MAC Client 上的网络流量。

配置链路聚合时请注意：

- 务必在配置链路聚合时避免网络上的广播风暴或回路，请提前禁用或断开所有您要操作的端口。待完成聚合链路的配置后再启用或连接这些端口。
- 每台 EDS-726 可以支持 4 组链路聚合组（设置为 Trk1, Trk2, Trk3, Trk4）。
- 各链路聚合组中可以添加 8 个端口。每个 LACP 链路聚合组最多配置 4 个备用端口，换句话说，就是每个 LACP 链路聚合组最多可以配置 12 个端口。
- 各链路聚合组中的各端口通信速率必须设置一致，如：100M Full, 100M Half, 10M Full 或 10M Half。这些端口的自侦测功能将被禁用。
- 只能采用全双工模式——只有在全双工模式下对 MAC 操作的点对点连接才支持链路聚合。
- 多路链路聚合——该项中指出的机制不支持 2 个以上系统之间的链路聚合。

在激活链路聚合设置的同时，一些高级功能会被禁用或被设定为出厂默认值：

- Port stat，如传输速率，双工方式以及流量控制会被设定为出厂默认值。
- Communication Redundancy 会被设置为出厂默认值。
- 802.1Q VLAN 会被设置为出厂默认值同时被禁用。
- Multicast Filtering 会被设置为出厂默认值。
- Port Lock 会被设置为出厂默认值同时被禁用。
- Set Device IP 会被设置为出厂默认值。
- Mirror Port 会被设置为出厂默认值同时被禁用。

配置链路聚合

从下图可以看出配置链路聚合时需要配置的一些参数。详细内容如下图所示。

Port Trunking Settings

Trunk Group: Trunk Type:

Member Ports

Port	Enable	Name	Speed	FDX Flow Ctrl

Up Down

Available Ports

Port	Enable	Name	Speed	FDX Flow Ctrl
<input type="checkbox"/> 1-1	Yes		Auto	Enable
<input type="checkbox"/> 1-2	Yes		Auto	Enable
<input type="checkbox"/> 1-3	Yes		Auto	Enable
<input type="checkbox"/> 1-4	Yes		Auto	Enable

Activate

步骤 1、从 Trunk Group 下拉框中选择 Trk1, Trk2, Trk3 或 Trk4。

步骤 2、从 Trunk Type 下拉框中选择 Static 或 LACP。

步骤 3、通过打勾来选择 Member Ports 和 Available Ports。

步骤 4、点击 Up/Down 按钮为链路聚合组添加或删除端口。

Trunk Group (Maximum of 4 trunk groups)

設置	说明	出厂设置
Trk1, Trk2, Trk3, Trk4	显示或指定链路聚合组 1, 2, 3, 4 的类型和端口	Trk1

Trunk Type

設置	说明	出厂设置
Static	指定为 Moxa 专有链路聚合协议	Static
LACP	指定为 LACP (IEEE 802.3ad, Link Aggregation Control Protocol)	Static

Member Ports/Available Ports

設置	说明	出厂设置
Member/Available Ports	点击 Up/Down 按钮为链路聚合组添加或删除端口	无
Check box	选择要添加或删除的端口	为选择
Port	端口号	无
Port description	显示各端口所连接的介质类型	无
Name	最大 63 各字符长度	无
Speed	显示传输速率 (100M-Full, 100M-Half, 10M-Full, or 10M-Half)	无
FDX Flow Control	显示端口 FDX 流控启用或禁用	无
Up	为链路聚合组添加端口	无
Down	为链路聚合组删除端口	无

Trunk Table

Trunk Group	Member Port	Status
Trk1 (Static)	2-1	Success
	2-2	Success
	2-3	Success
	2-4	Success
Trk2 (LACP)	3-1	Success
	3-2	Success

Trunk Table

設置	说明
Trunk Group	显示链路聚合类型和组
Member Port	显示从属于组的端口
Status	Success 是指链路聚合工作正常。 Fail 是指链路聚合工作异常。 Standby 是指该端口为备用端口。若链路聚合组包含有 8 个以上的端口，则第 9 个端口即为备用端口

配置 SNMP

EDS-726 支持 SNMP V1/V2c/V3。SNMP V1 和 SNMP V2c 使用一组字符串来进行认证，也就是说 SNMP 服务器可以访问所有对象，根据不同的字符串用户具有不同的权限。如 public 权限为只读，而 private（默认值）为读/写。SNMP V3 要求用户选择 MD5 或 SHA 中的一种认证方式，它是最安全的一种协议。您也可以通过对数据加密来提升数据传输的安全级别。

下表所示为 EDS-726 所支持的 SNMP 安全模式和安全级别。请选择用于 SNMP 客户端和服务端通信时所采用的安全模式和安全级别。

协议版本	安全模式	认证类型	数据加密	方式
SNMP V1, V2c	V1, V2c Read Community	Community string	无	Community string 匹配认证
	V1, V2c Write/Read Community	Community string	无	Community string 匹配认证
SNMP V3	No-Auth	No	无	利用 admin/user 帐户来访问对象
	MD5 or SHA	MD5 or SHA	无	基于 HMAC-MD5 或 HMAC-SHA 算法的认证, 认证的最低要求为 8 位密码
	MD5 or SHA	MD5 or SHA	Data encryption key	基于 HMAC-MD5 或 HMAC-SHA 算法和数据密钥的认证, 认证和数据加密的最低要求为 8 位密码和密钥

这些参数可以通过 SNMP 页面来配置。更多有关参数设置的详情请参考下图。

The screenshot shows the SNMP configuration interface with the following settings:

- SNMP Versions:** V1, V2c
- V1, V2c Read Community:** public
- V1, V2c Write/Read Community:** private
- Admin Auth. Type:** No-Auth
- Admin Data Encryption Key:** (checkbox unchecked)
- User Auth. Type:** No-Auth
- User Data Encryption Key:** (checkbox unchecked)
- Trap Settings:**
 - Trap Server IP/Name: (empty)
 - Trap Community: public
- Private MIB information:** enterprise.8691.7.1
- Activate:** (button)

SNMP 读/写设置

SNMP Versions

设置	说明	出厂设置
V1, V2c, V3 or V1, V2c or V3 only	选择用于管理交换机的 SNMP 协议版本	V1, V2c

V1, V2c Read Community

設置	说明	出厂设置
V1, V2c Read Community	使用最多30个字符的community string匹配来认证。SNMP服务器可以访问所有对象，但它使用community string public，具备只读的权限	Public

V1, V2c Write/Read Community

設置	说明	出厂设置
V1, V2c Read/Write Community	使用最多 30 个字符的 community string 匹配来认证。SNMP 服务器可以访问所有对象，但它使用 community string private，具备读写的权限	Private

对于 SNMP V3，访问 EDS-726 的帐户有两级优先权，Admin 帐户可以访问并且能读/写 MIB 文件，而 User 帐户只能读 MIB 文件，不能写。

Admin Auth. Type (for SNMP V1, V2c, V3, and V3 only)

設置	说明	出厂设置
No-Auth	使用 admin 帐户登陆，无需认证	无
MD5-Auth	采用 HMAC-MD5 算法认证。认证的最低要求为 8 个字符的密码	无
SHA-Auth	采用 HMAC-SHA 算法的认证。认证的最低要求为 8 个字符的密码	无

Admin Data Encryption Key (for SNMP V1, V2c, V3, and V3 only)

設置	说明	出厂设置
Enable	数据加密的最低要求是 8 个字符长度的密钥（最多 30 个字符）	无
Disable	无数据加密	无

User Auth. Type (for SNMP V1, V2c, V3 and V3 only)

設置	说明	出厂设置
No-Auth	使用 admin 帐户登陆，无需认证	无
MD5-Auth	采用 HMAC-MD5 算法认证。认证的最低要求为 8 个字符的密码	无
SHA-Auth	采用 HMAC-SHA 算法的认证。认证的最低要求为 8 个字符的密码	无

User Data Encryption Key (for SNMP V1, V2c, V3 and V3 only)

設置	说明	出厂设置
Enable	数据加密的最低要求是 8 个字符长度的密钥（最多 30 个字符）	无
Disable	无数据加密	无

Trap 设置

Trap Server IP/Name

設置	说明	出厂设置
IP or Name	输入网络上 Trap Server 的 IP 地址或名字	无

Trap Community

設置	说明	出厂设置
Character string	使用 community string 匹配来进行认证 (最多 30 个字符)	Public

Private MIB 信息

Switch Object ID

設置	说明	出厂设置
8691.7.1	EDS-726 的企业值	Fixed

注意：不能更改 Switch Object ID。

通信冗余功能

在网络中设置通信冗余功能可以保护关键的连接以免出错，避免 network loops，将网络中断时间缩减至最小。

通信冗余功能允许用户设置网络中冗余 loops，在线缆断开或损坏的时候提供备用数据传输路由。对于工业应用来说这是很重要的特点，因为需要花上几分钟时间定位断开或损坏的线缆。举个例子来说，假如 MOXA EDS-726 是生产线上关键的通信设备，几分钟的停工时间会造成巨大的损失。MOXA EDS-726 有两个不同的协议来支持通信冗余功能——Rapid Spanning Tree Protocol (IEEE 802.1w) 和 Turbo Ring。

Turbo Ring and STP/RSTP 不能在网络中同时使用，下表列出了两者的一些关键的不同点。您可以根据您的需要来决定哪种特性最适合您的网络。

	Turbo Ring	STP	RSTP
Topology	Ring	Ring, Mesh	Ring, Mesh
Recovery Time	< 300 ms	Up to 30 sec.	Up to 5 sec

千兆冗余以太网环网自愈能力 (< 300 ms)

以太网已经成为工业自动化应用中普遍的数据通信方式。实际上，以太网在集成视频、声音和高速工控数据传输中的运用是十分广泛的。MOXA EDS-726 配备了 Gigabit Turbo Ring 的冗余千兆以太网协议，为系统管理员设置灵活稳定的千兆以太网网络提供了极其方便的途径。有了 Gigabit Turbo Ring，就算在网络任何地方断线的情况下，仍然可以保证您的自动化系统在 300ms 内恢复正常通信。

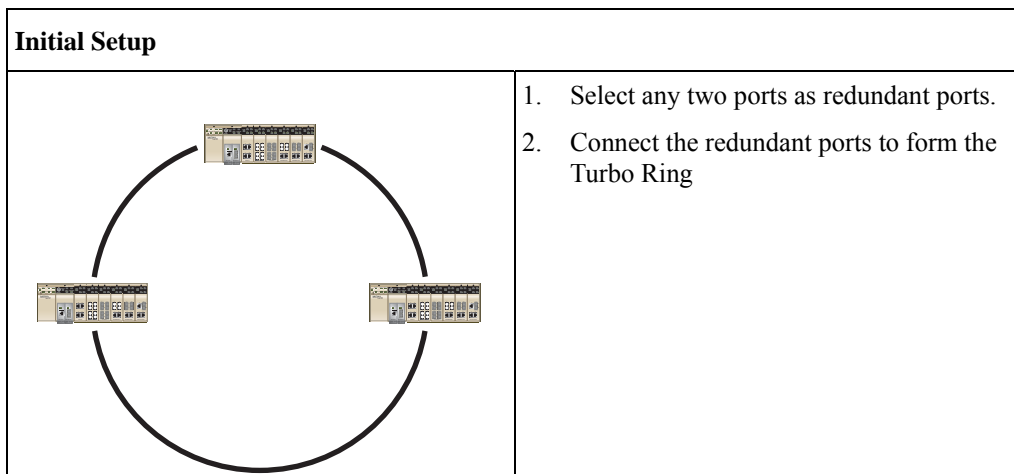


注意： 在设置骨干网络时可以同时启用链路聚合和 Turbo Ring，这样一来，不但增加网络带宽的还为系统提供了冗余功能。例如，假设将端口 1 和 2 设置为链路聚合组 Trk1，在将 Trk1 设置为 Turbo Ring。若端口 1 连接失败，余下的端口 2 将会分担网络上的流量。若端口 1 和 2 连接都失败，Turbo Ring 就会在 300ms 内启用备用路径来恢复通信。

Turbo Ring 的概念

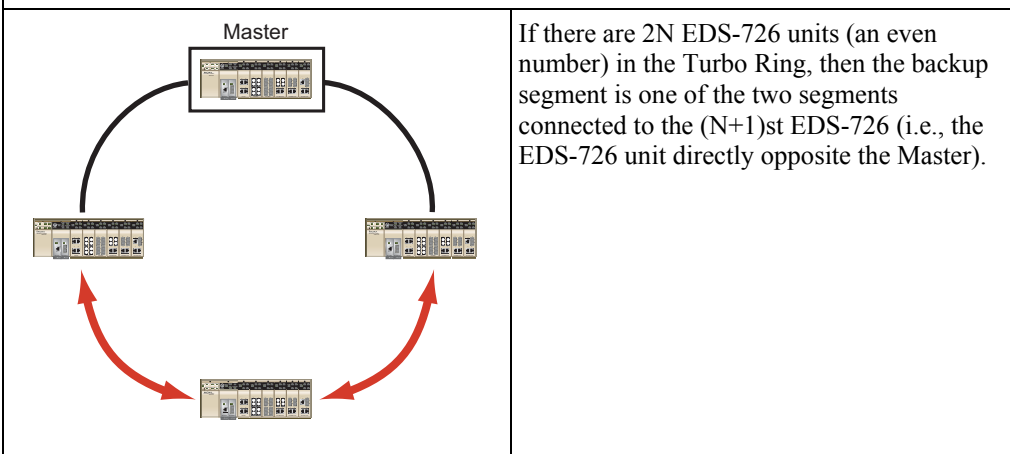
MOXA 公司自主开发的 Turbo Ring 协议在很大程度上优化了通信冗余功能，并保证网络的恢复时间更短。

Turbo Ring 协议指定网络中的以太交换机作为主机，阻止网络中任意冗余环的数据包。当环网中的某个分支和其余网络断开的时候，Turbo Ring 协议能自动重新调整环网，所以断开的网络能和其他网络重新建立连接。

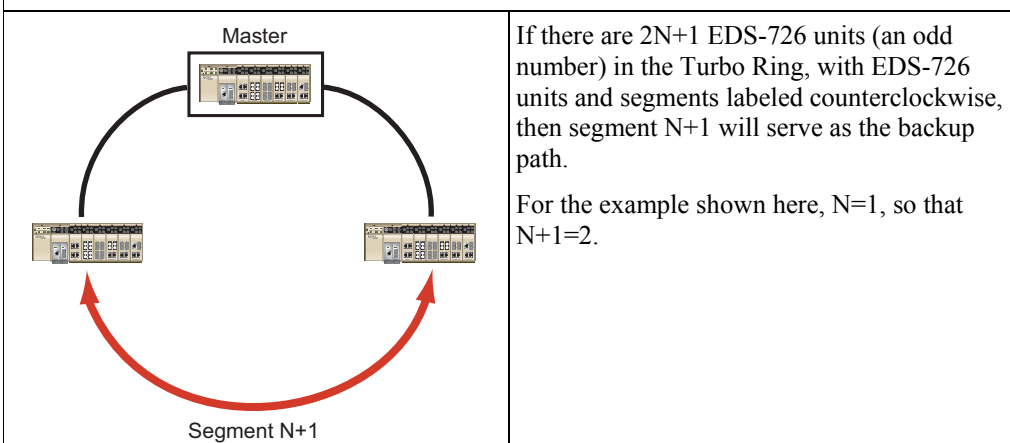


客户使用 Turbo Ring 的时候不需要设定主机，主机只是用来区分哪个段用作备用路径。冗余环的实际拓扑结构，也就是说哪端线路将被阻止是由构成环网的 EDS-726 数量和环网主机的位置决定。

环网上 EDS-726 交换机的数目为偶数时



环网上的 EDS-726 交换机的数目为奇数时

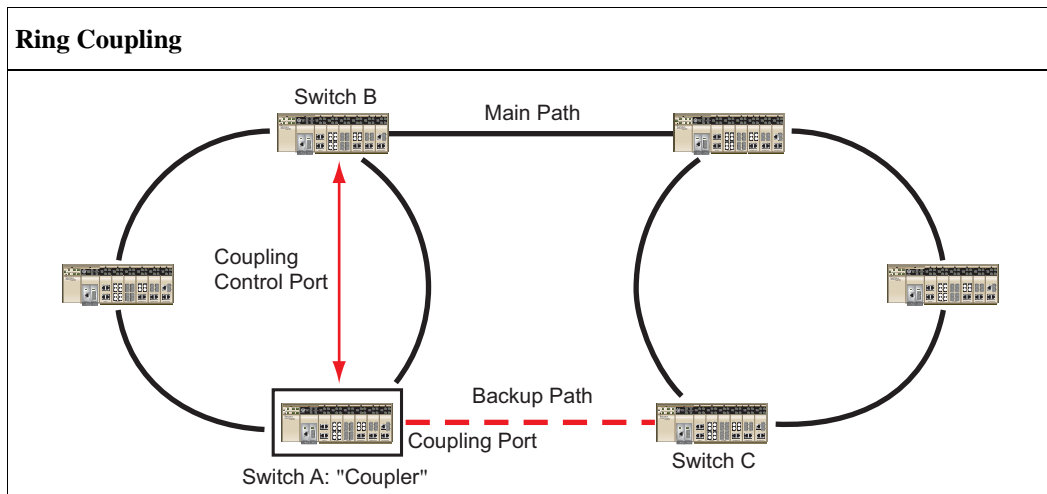


对某些系统而言，设备与设备之间的距离比较远，要将所有的设备连接起来形成一个大的冗余环网可能不太现实。而 Turbo Ring 提供的环网耦合功能可以帮助您将那些分散的设备组合为一些小的冗余环网，同时还可以实现各环网之间的通信。下图演示了两个 Turbo Ring 之间的耦合过程。



注意

在 VLAN 中，您必须将“Redundant port”，“Coupling Port”和“Coupling Control Port”设置为“Trunk Port”。因为这些端口作为骨干网络，担负着传输所有不同 VLAN 到不同 EDS-726 封包的任务。



为了支持环间耦合功能，选择 Turbo Ring 中的一个 EDS-726（如上图中的 Switch A），进入通信冗余功能页面开启 Ring Coupling。选择一个端口作为耦合端口，然后将相邻耦合环网中相对的任意 EDS-726 端口连接起来。在选择一个端口作为耦合控制端口，和相同环网中相邻的任意 EDS-726（如 Switch B）的端口连接起来，耦合交换机（Switch A）将通过耦合控制端口监视 Switch B 的状态，以决定耦合控制端口的备用路径是否要被恢复。



注意

用户只需要开启一台 EDS 上的耦合环网功能（不是相对的或相邻的 EDS-726），在四个单独的端口中需要设置 Redundant Port，Coupling Port 和 Coupling Control Port。

注意：

环间耦合和环网主机不需要在同一台 EDS-726 中设置。

设置 Turbo Ring

从下图可以看出需要设置哪些 Turbo Ring 协议参数。详细内容如下：

Now Active

该栏显示当前使用那种通信协议：Turbo Ring, RSTP/STP 或是没有默认值。

Master/Slave

该栏只有当选择工作在 Turbo Ring 模式下才会出现，显示该 EDS-726 是否作为 Turbo Ring 中的主机。

注意： 用户使用 Turbo Ring 时不需要设置主机，只需要指定主机是用来决定哪一段作为备用路径。如果用户没有为 Turbo Ring 指定一个专门的主机，则交换机之间会自动选择出一台做主机。

Redundant Port Status

该栏显示当前冗余端口的状态。正常传输为 Forwarding，如果该端口作为备用路径停止传输则为 Blocked，端口无连接时为 Link Down。

Ring Coupling

显示 Ring Coupling 功能是开启还是禁止。

Coupling Port Status

该栏显示当前耦合端口的状态。正常传输为 Forwarding，如果该端口作为备用路径停止传输显示 Blocked，无连接时为 Link Down。

在页面的底部，用户可以设置这个功能—Settings。对于 Turbo Ring，用户可以设置：

Redundancy Protocol

設置	说明	出厂设置
Turbo Ring	选择此项切换到 Turbo Ring 设置页面	无
RSTP (IEEE 802.1W/1D)	选择此项切换到 RSTP 设置页面	无

Set as Master

設置	说明	出厂设置
Enable/Disable	选择该 EDS-726 作为主机	无

Redundant Ports

設置	说明	出厂设置
1st Port	选择 EDS-726 的任何端口作为冗余端口	Port 7 (如果开启 Turbo Ring)
2nd Port	选择 EDS-726 的任何端口作为冗余端口	Port 8 (如果开启 Turbo Ring)

Enable Ring Coupling

設置	说明	出厂设置
Enable/Disable	选择该 EDS-726 作为耦合器	无

Coupling Ports

設置	说明	出厂设置
Coupling Port	选择 EDS-726 的任何端口作为耦合端口	Port 5 (如果开启 Turbo Coupling)
Coupling Control Port	选择 EDS-726 的任何端口作为耦合控制端口	Port 6 (如果开启 Turbo Coupling)

STP/RSTP 的概念

Spanning Tree 协议可以使你的网络在抵抗链接故障方面更有弹性, 而且提供对 loops 的保护-这是网络风暴产生的主要原因。EDS-726 中是默认禁止 STP 的, 为了最大提高有效性, 应该把网络中所有 EDS-726 的 RSTP/STP 开启。

Rapid Spanning Tree 协议 (RSTP) 是 STP 的升级版。RSTP 由 IEEE Std 802.1w-2001 定义, 执行 Spanning Tree 算法和协议。RSTP 的优点如下:

- 在网桥互连网络中更快的拓扑决策能力。
- 在继承网络中通过后向兼容可以更容易的进行配置。
 - 将在某一个端口默认发送 802.1D 形式的 BPDU, 如果接收到的数据包也是这种格式。
 - EDS-726 上的一些端口可以工作在 RSTP(802.1w)模式, 另外一些端口如连接到继承交换机上的可以工作在 STP(802.1D)模式。

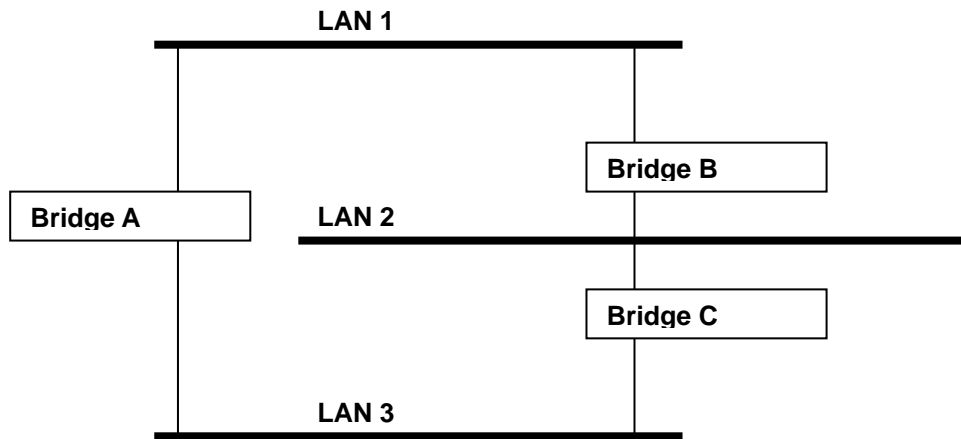
注意: RSTP 的功能和 STP 一样, 两者具体的区别参看本章 How RSTP diff from STP 部分。接下来将利用网桥替代交换机进行阐述。

什么是 STP?

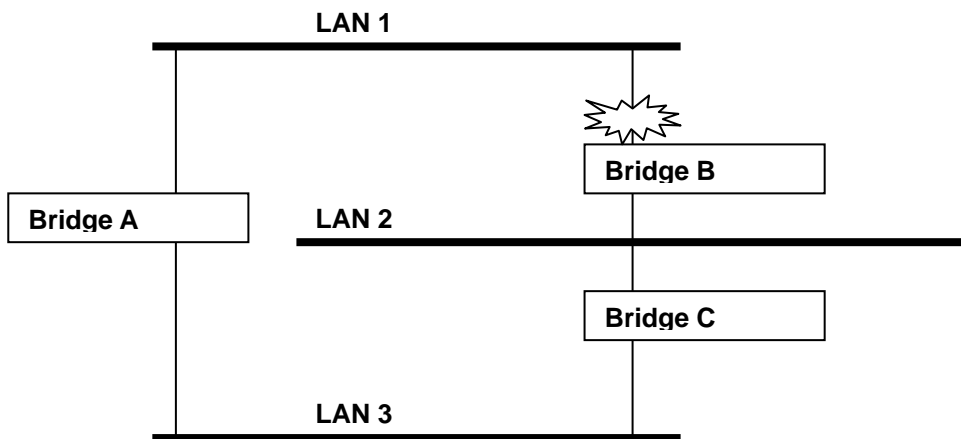
STP (802.1D)基于网桥的系统，允许对网络流量并行传输且使用 loop 来检测：

- 查找并禁止低效路径（即低带宽路径）。
- 当大多数高效路径出现故障时开启一条低效路径。

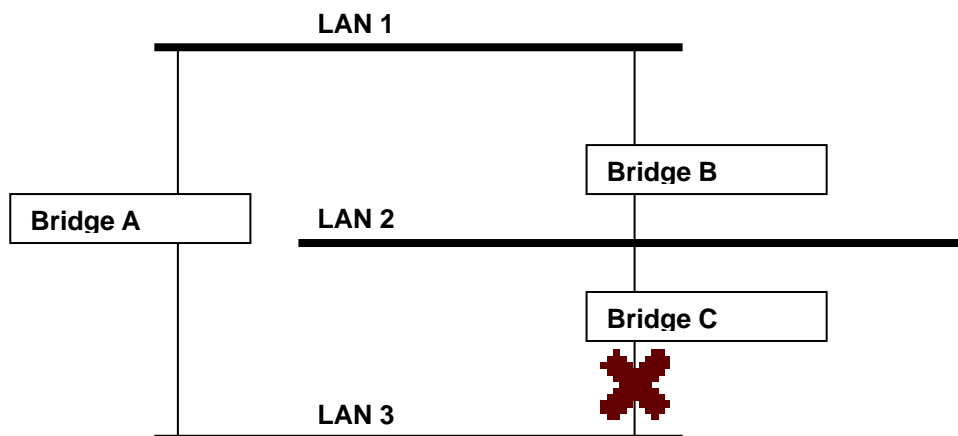
举例说明，下图是用 3 个网桥将一个网络分成 3 个网段。通过此项设置，每个网段有两条路径和其他网络进行通信。如果 STP 没有开启，那此项设置将产生 loops 从而造成网络过载。



下图是在设置中将网桥 STP 开启的结果。STP 检测两条路径，禁止其中的一条前向传输数据，所以能很好的运行。打个比方来说，STP 能够决定从网段 2 到网段 1 的数据流量应该流经网桥 C 和 A，因为该路径有更大的带宽，效率更高。



如果检测到链接发生故障，如下图所示，STP 进程将重新设置网络，所以来自网段 2 的流量将流经网桥 B。



STP 决定每个网桥段之间的路径是最有效的，并且在网络中指定一个特殊的参考点。一旦检测到最有效路径，其他路径都将被阻塞。因此，从以上 3 幅图中可以看出，STP 一开始决定了通过网桥 C 的路径是最有效的，那么通过网桥 B 的路径将被阻塞。在检测到网桥 C 有故障发生后，STP 重新估计形势打开通过网桥 B 的路径。

STP 工作原理

当 STP 开启后，将为网络中的流量选择最合适的路径。具体方法将在以下部分介绍。

STP Requirements

在 STP 能够配置网络之前，STP 系统需要：

- 在所有的网桥之间进行通信。通信是由通过 BPDU 实现的，其中 BPDU 和已知的 Multicast 地址一起被分组发送。
- 每个网桥必须有一个网桥标志符，以此来区分哪个网桥是作为 STP 系统的中心参考点或 root 网桥—网桥标志符较低的一般被指定为 root 网桥。网桥标志符是由网桥的 MAC 地址和为网桥定义的优先级计算出来的。EDS-726 默认的优先级是 32768。
- 每个端口有一个开销用来区分每个链接的效率—一般是由链接的带宽来决定的，开销越高，链接的效率越低。下表给出了交换机默认的端口开销。

Port Speed	Path Cost 802.1D, 1998 Edition	Path Cost 802.1w-2001
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1000 Mbps	4	20,000

STP 计算

STP 进程的第一步为计算，在该步骤中，每个网桥通过发送 BPDU 来让 STP 计算：

- 哪个网桥应该作为 root 网桥。Root 网桥用作网络配置的中心参考点。
- 每个网桥的 root 路径开销—就是每个网桥到 root 网桥路径的开销。
- 每个网桥的哪个端口应该用作 root 端口。Root 端口是连接到 root 网桥的最有效的端口，也就是说有最低的 root 路径开销。必须注意的是 root 网桥没有 root 端口。

- 哪个网桥作为每个网段的指定网桥。指定网桥从网段开始具有最低的 root 路径开销，如果几个网桥具有相同的 root 路径开销，那么具有最低网桥标志符的网桥将作为指定网桥。所有的数据流量将从 root 网桥流向指定网桥。网桥上连接到网段的端口成为指定网桥端口。

配置 STP

当所有网桥统一好在 root 网桥上的标志符，并且设置好其他相关参数后，每个网桥只在各自网段中的 root 端口和指定网桥端口之间转发数据。而其他的端口将被阻止，这就以为着这些端口即不能发送也不能接收。

重新配置 STP

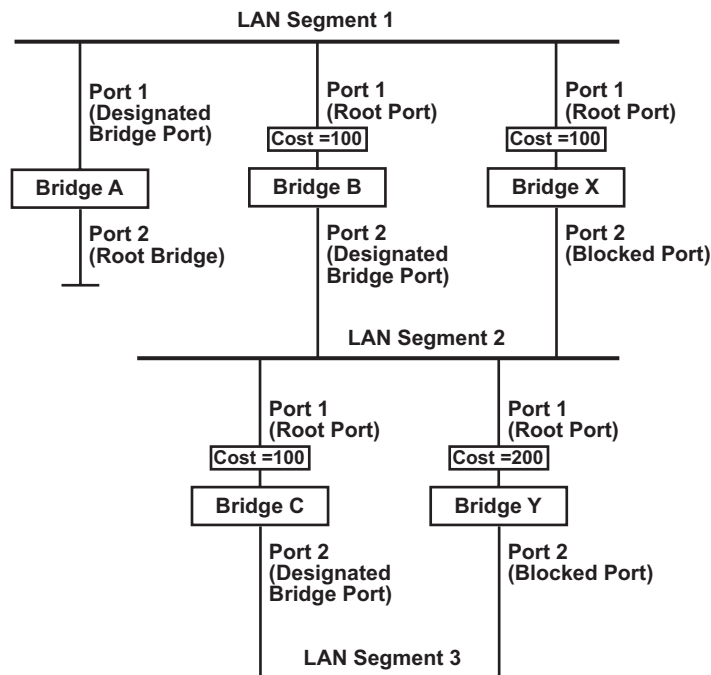
当网络拓扑达到稳定后，所有的网桥接收从 root 网桥定时发出的 Hello BPDU。如果某网桥在某一定时间间隔（the MAX Age Time）内没有收到该信息，该网桥就假定 root 网桥或者它自身和 root 网桥之间的链接发生故障。然后网桥就重新配置网络进行改变。如果你已经设置好一个 SNMP trap destination，当网络拓扑发生改变时，第一个检测到变化的网桥发出一个 SNMP trap。

RSTP 和 STP 的不同点

RSTP 和 STP 的工作方式类似，但是在 BPDU 中包含了额外的信息。该信息能够让每个网桥开启和相邻网桥之间的链接的时候确认已经采取措施阻止 loop 的形成。这可以使相邻网桥之间通过点对点的方式建立链接，而不需要等待来保证网络中的其余网桥有时间对改变作出反应。所以 RSTP 的主要优点是在本地决定设置而不是在整个网络中，这也就是为什么 RSTP 能够自动设置，而且相对 STP 具有更快的恢复链接时间。

STP 举例

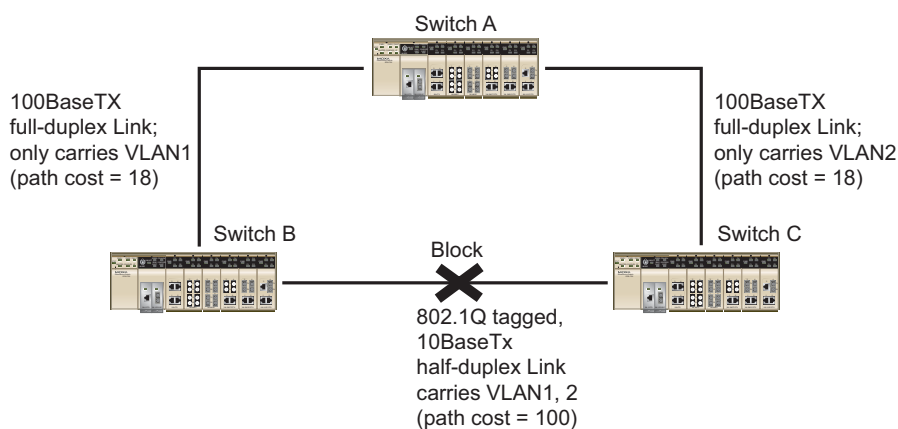
下图是一个已经开始 STP 的 LAN，分成三段，各个段之间通过两个可能的链接连接在一起。



- 网桥 A 在网络中的标志符最低，因此被选作 root 网桥。
- 因为网桥 A 是 root 网桥，所以也是网段 1 的指定网桥。因此网桥 A 上的端口 1 被选作为网段 1 的指定网桥端口。
- 网桥 B,C,X 和 Y 上的端口 1 被定义为 root 端口，因为它们离 root 网桥最近，路径效率最高。
- 网桥 B 和 X 为网段 2 提供相同的 root 路径开销。然而网桥 B 被选作网段的指定网桥因为它的标志符更低。网桥 B 上的端口 2 因此被选作网段 2 的指定网桥端口。
- 网桥 3 被选作网段 3 的指定网桥，因为它为网段 3 提供最低的 root 路径开销。
 - 网桥 B 到 C 的路径开销为 200 (C to B=100, B to A=100)
 - 网桥 Y 到 C 的路径开销为 300 (Y to B=200, B to A=100)
- 网桥 C 的端口 2 因此被选作网段 3 的指定网桥端口。

在多个 VLAN 网络中使用 STP

IEEE Std 802.1D, 1998 Edition 在计算 STP 信息时并没有考虑 VLAN，只是在物理连接的基础上进行计算。因为这个原因，一些网络配置能够通过 STP 系统分成若干个独立的部分构成 VLAN。因此，你必须保证你网络中的任何 VLAN 配置考虑期望拓扑和替代拓扑，那将可能导致链接故障。举例来说，下图是一个包括 VLAN1 和 2 的网络，他们在交换机 B 和 C 之间通过 802.1Q 标记的链接进行连接。默认情况下该链接的端口开销为 100 将被阻止因为其他交换机到交换机之间链接的端口开销为 36 (18+18)。这就意味着现在所有 VLAN 都被分离开来来了，交换机 A 和 B 上的 VLAN 1 不能和交换机 C 上的 VLAN1 通信，交换机 A 和 C 上的 VLAN2 也不能和交换机 B 上的 VLAN2 通信。



为了避免任何 VLAN 再被分，我们建议所有交换机之间的连接按照 802.1QVLAN 标准进行连接来保证连接的不中断。打个比方来说，交换机 A 和 B 之间的连接以及交换机 A 和 C 之间的连接应该是 802.1Q 标记的并且通过传送 VLAN 1 和 2 来保证连接。

关于 VALN 标记更详细的信息，参看 VLAN 设置部分。

设置 STP/RSTP

从下图可以看出需要设置哪些 STP 协议参数。详细内容如下：

Communication Redundancy

Current Status

Now Active: **None**
 Root/Not root: ---

Settings

Redundancy Protocol: RSTP (IEEE 802.1W/1D)

Bridge Priority: 32768 Hello Time: 2 (10ms)
 Forwarding Delay: 15 (10ms) Max Age: 20 (10ms)

Port	Enable RSTP	Port Priority	Port Cost	Status
1-1	<input type="checkbox"/>	128	200000	---
1-2	<input type="checkbox"/>	128	200000	---
1-3	<input type="checkbox"/>	128	200000	---
1-4	<input type="checkbox"/>	128	200000	---
2-1	<input type="checkbox"/>	128	200000	---
2-2	<input type="checkbox"/>	128	200000	---

Activate

在该页面的顶部，用户可以检查这项功能的状态。对于 RSTP，你将看到：

Now Active:

该栏显示当前使用那种通信协议：Turbo Ring, RSTP, 或没有。

Root/Not Root

该栏只有当选择工作在 RSTP 模式下才会出现，显示该 EDS-726 是否是 Spanning Tree 的 Root。

在页面的底部，用户可以设置这个功能—Settings。对于 RSTP，用户可以设置：

Protocol of Redundancy

設置	说明	出厂设置
Turbo Ring	选择此项切换到 Turbo Ring 设置页面	无
RSTP (IEEE 802.1W/1D)	选择此项切换到 RSTP 设置页面	无

Bridge priority

設置	说明	出厂设置
用户可选数字	选择更低的数字来提高该设备的网桥优先级。高优先级的网桥更容易被设为 Spanning Tree 拓扑的 root。	32768

Hello time (sec.)

設置	说明	出厂设置
用户可调数字	Spanning Tree 拓扑的 root 周期性的向网络中的其他设备发出 Hello 信息来检查拓扑是否正常。Hello time 是 root 发送信息的等待时间。	2

Max. Age (sec.)

設置	说明	出厂设置
用户可调数字	如果不是 root 的设备在最大为 Max Age 的时间内没有收到 hello 信息，该设备将重新配置将自己设为 root。一旦网络中出现两个以上 root 时，设备将重新调整建立新的 Spanning Tree 拓扑。	20

Enable STP per Port

設置	说明	出厂设置
Enable/Disable	开启端口作为 Spanning Tree 拓扑的一个节点。	Disabled

注意： 我们建议当端口连接到网络相对设备上时不要启用 Spanning Tree 协议，因为这将造成不必要的调整。

Port Priority

設置	说明	出厂设置
用户可选数字	选择更低的数字来提高该端口的优先级作为 Spanning Tree 拓扑的一个节点。	128

Port Cost

設置	说明	出厂设置
用户可调数字	输入更高的代价来表明该端口不适合用作 Spanning Tree 拓扑的一个节点。	200000

Port Status

显示端口的当前 Spanning Tree 状态，Forwarding 为正常发送，Blocked 禁止发送。

Configuration Limits of RSTP/STP

我们应该指出 Spanning Tree 算法在下面列出的三个变量上存在约束性。

[Eq. 1]: $1 \text{ sec} \leq \text{Hello Time} \leq 10 \text{ sec}$

[Eq. 2]: $6 \text{ sec} \leq \text{Max. Age} \leq 40 \text{ sec}$

[Eq. 3]: $4 \text{ sec} \leq \text{Forwarding Delay} \leq 30 \text{ sec}$

这三个变量服从以下两个不等式:

$$[\text{Eq. 4}]: 2 * (\text{Hello Time} + 1 \text{ sec}) \leq \text{Max. Age} \leq 2 * (\text{Forwarding Delay} - 1 \text{ sec})$$

如果违反了这些约束条件, MOXA EDS-726 固件会立即发出警告。例如, 设置:

Hello Time = 5 sec, Max. Age = 20 sec, and Forwarding Delay = 4 sec 没有违反约束条件 1, 2, 3, 但是违反了约束条件 4。

因为: $2 * (\text{Hello Time} + 1 \text{ sec}) = 12 \text{ sec}$, and $2 * (\text{Forwarding Delay} - 1 \text{ sec}) = 6 \text{ sec}$ 。

你可以修正其中任意的变量值来满足约束条件。一个简单的办法就是提高 Forwarding Delay 值, 至少要 11sec。

流量优先级功能

流量优先级功能通过提高数据传输的可靠性来为你的网络提供 QoS, 你可以在网络中给流量设定优先级来使高优先级的数据传输有最小的时延。通过设定一些规则来控制流量, 从而满足网络的 QoS 要求。规则定义了不同的流量类型, 通过区分类型来决定哪些类型的流量可以通过交换机。MOXA EDS-726 能够检查 IEEE 802.1p/1Q layer 2 CoS 标志, 甚至 layer 3 TOS 信息, 从而提供整个网络分类的一致性。MOXA EDS-726 的 QoS 能力提高了恶劣环境下工业网络的性能和决策能力。

流量优先级的概念

什么是流量优先级

当今的应用流量包含了不同的数据类型。当这些不同类型的数据竞争相同的带宽时, 网络会迅速过载, 导致响应时间变慢 (长响应时间) 和程序暂停。流量优先级是一种给数据赋予不同优先级的机制, 所以那些时间敏感和系统紧急数据能够在网络中被平稳传送并且时延最小。流量优先级的优点如下:

- 你可以控制网络中各种流量以及管理出现的网络拥塞, 因此提高了性能。
- 你可以为流量指定优先级, 给那些时间紧急和商业紧急应用设定高优先级。
- 你可以为多媒体应用如视频会议以及 IP 电话提高预期吞吐量, 最小化流量时延和抖动。
- 你可以在流量增加的时候提高网络性能, 也就减少了不断增加网络带宽的需求, 节省了开销。

流量优先级是怎样工作的

流量优先级利用 EDS-726 中的四个流量队列来保证不同队列中高优先级的流量先于低优先级流量被转发。为你的网络提高 QoS。

EDS-726 流量优先级依赖于两个工业标准的方法:

- **IEEE 802.1D**—第二层 marking scheme
- **Differentiated Services (DiffServ)**—第三层 marking scheme.

IEEE 802.1D Traffic Marking

IEEE Std 802.1D, 1998 Edition marking scheme 是 IEEE Std 802.1D 的加强版, 在 LAN 中启用 QoS。流量服务级别定义为 IEEE 802.1Q 的 4 字节标记, 用来携带 VLAN 标志符以及 IEEE 802.1P 优先级信息。4 字节标志紧跟在目的 MAC 地址和源 MAC 地址后面。

IEEE Std 802.1D, 1998 Edition marking scheme 为每个帧指定一个 0 到 7 之间的 802.1P 优先级, 那就决定了某种流量类型应有的服务级别。参考下表的例子, 不同的流量类型怎样对应 8 个 802.1P 优先级。

IEEE 802.1p Priority Level	IEEE 802.1D Traffic Type
0	Best Effort (default)
1	Background
2	Standard (spare)
3	Excellent Effort (商业紧急)
4	Controlled Load (流媒体)
5	Video (互动媒体); less than 100 milliseconds of latency and jitter
6	Voice (互动语音); less than 10 milliseconds of latency and jitter
7	Network Control Reserved traffic

尽管 IEEE 802.1D 标准是 LAN 环境下使用最广泛的优先级方案，仍然有一些限制条件：

- 在帧结构中需要额外的 4 字节标记，一般在以太网中是可选项，如果没有这个标记，scheme 将不能工作。
- 标记是 IEEE 802.1D 报头的一部分，所以在第二层执行 QoS，整个网络需要执行 IEEE 802.1D 标记。

只有 LAN 和没有交叉路由的 WAN 链接支持该方案，因为 IEEE 802.1D 标记在经过路由器的时候会被除去。

Differentiated Services (DiffServ) Traffic Marking

DiffServ 是第三层的 marking scheme，用 IP 报头中 DiffServ Code Point (DSCP) 来保存数据包的优先级信息。DSCP 是一种高级智能的流量标记方法，因为你可以选择怎样设置网络中不同流量类型的优先级。DSCP 使用 64 个值来对应用户定义的服务级别，可以让你确立更多的对网络流量的控制。

IEEE 802.1D DiffServ 的优点：

- 你可以配置你的交换机怎么对待被选择的应用和流量类型，给它们指定不同的网络服务级别。
- 数据包中不需要额外的标记。
- DSCP 使用数据包中的 IP 报头，因此可以在 internet 中保存优先级。
- DSCP 能和 IPV4 TOS 后向兼容，这就使得现有设备可以使用第三层 TOS 允许的优先级方案。

流量优先级

EDS-726 是在 OSI7 层模型第三层的基础上对流量进行分类，交换机对接收到的流量区分优先次序是根据接收到的数据包中定义的优先级信息。到来的流量在 IEEE 802.1D 帧的基础上被分类并根据数据包中定义的 IEEE 802.1p 服务级别分配到合适的优先级队列。服务优先级标记（值）定义在 IEEE 802.1Q 4 字节标记中，因此如果网络按照 VLAN 以及 VLAN 标记被配置，那么流量中只包含 802.1p 优先级标记。流量将按如下方式流经交换机：

1. EDS-726 接收到的数据包不一定和 802.1p 标记有联系，如果没有联系，数据包将被赋一个默认的 802.1p 标记（通常是 0）。如果有，数据包将被重新赋一个 802.1p 值，这将导致所有旧的 802.1p 标记信息丢失。
2. 因为 802.1p 优先级是固定在优先级队列上的，数据包将放到合适的优先级队列中，等待从后世的出端口发送出去。当数据包到达队列的首部时将被发送，设备决定是否 VLAN 标记出端口，如果是的话，那么新的 802.1p 标记将用在扩展的 802.1D 头部。

EDS-726 为了 802.1D 流量分类将检查从进入端口接收到的数据包，然后根据标记中 802.1p 值给数据包赋上优先级。是 802.1p 值决定数据包映射到哪个流量队列的。

流量队列

EDS-726 的硬件有多个流量队列来对数据包进行排序。更高优先级的数据包能通过 EDS-726 而不需要被低优先级的数据包延时，当每个数据包到达 EDS-726 后，经过输入端口处理（包含分类，标记/重新标记），将分类送到合适的队列中。然后交换机将每个队列中的数据包转发出去。

EDS-726 支持两种不同的队列排序机制：

- **Weight fair:** 所有流量队列均可采用该机制，高级别的队列具有优先级。在大多数情况下是按照优先级高低的顺序来执行的，只有在较高优先级的流量超过网络容量时优先级较低的流量才可以通过。
- **Strict:** 该方式适用于流量较大的队列；优先级较低的队列通常被延时直到那些优先级较高的队列被发送完毕。

配置流量优先级

QoS 提供了流量优先的功能，确保重要数据安全可靠地进行传输。EDS-726 系列交换机通过检测 IEEE 802.1p/1Q 第二层中的 CoS 标签以及第三层中的 TOS 信息来实现整个网络分类的一致性。EDS-726 系列所具备的 QoS 能力大大提升了工控网络的性能，并决定数据传输的优先级。

QoS 分类

QoS Classification

Queueing Mechanism: Weight Fair(8:4:2:1)

Port Group	Inspect ToS
Group1 (2-1,2-2,2-3,2-4)	<input checked="" type="checkbox"/>

Port	Inspect CoS	Default Port Priority
2-1	<input checked="" type="checkbox"/>	3(Normal)
2-2	<input checked="" type="checkbox"/>	3(Normal)
2-3	<input checked="" type="checkbox"/>	3(Normal)
2-4	<input checked="" type="checkbox"/>	3(Normal)

Activate

MOXA EDS-726 支持对 layer 3 TOS and/or layer 2 CoS 标记信息检查来决定怎样对流量数据包分类。

Queuing Mechanism

設置	说明	出厂设置
Weighted Fair	EDS-726 有四个优先级队列, 在加权公平方案中, 8, 4, 2, 1 权重用作四个优先级。这样就避免低优先级帧被剥夺发送机会, 只是被高优先级帧延迟一下。	Weighted
Strict	在严格优先级方案中, 所有优先级最高的帧从端口发送出去直到优先级队列为空, 然后下一优先级队列发送。这样低优先级队列就不能发送任何帧, 但是可以保证高优先级帧能够尽快发送。	

Inspect TOS

設置	说明	出厂设置
Enable/Disable	检查复选框来开启 EDS-726 的检查 TOS 功能, 该功能是通过检查 IPV4 帧的服务类型 (TOS) 位来决定每帧的优先级。	Enable

Inspect CoS

設置	说明	出厂设置
Enable/Disable	检查复选框来开启 EDS-726 的检查 TOS 功能, 该功能是通过检查 MAC 帧的 802.1p CoS 标志来决定每帧的优先级。	Enable

Default Port Priority

設置	说明	出厂设置
Low/Normal/ Medium/High	给不同优先级队列的输入帧设定默认的端口优先级。如果接收到的数据包没有包含任何标志信息 (TOS, CoS), 默认端口优先级将起作用。	Normal

注意: 输入帧的优先级是按照以下顺序决定的:

1. 检查 TOS
2. 检查 CoS
3. 默认的端口优先级。

注意: 设计者可以单独或按照一定组合开启分类功能。举个例子来说, 如果网络设计需要一个高优先级的端口, 那么就关闭检查 TOS 和检查 CoS 功能, 只开启默认端口优先级功能, 那样该端口所有输入帧都将赋上相同的优先级。

CoS Mapping

Mapping Table of CoS Value and Priority Queues

CoS	Priority Queue
0	Low
1	Low
2	Normal
3	Normal
4	Medium
5	Medium
6	High
7	High

Activate

設置	说明	出厂设置
Low/Normal/ Medium/High	设置 CoS 值和 4 个输出队列的映射表。	0: Low 1: Low 2: Normal 3: Normal 4: Medium 5: Medium 6: High 7: High

TOS/DiffServ Mapping

Mapping Table of ToS (DSCP) Value and Priority Queues

ToS	Level	ToS	Level	ToS	Level	ToS	Level
0x00(1)	Low	0x04(2)	Low	0x08(3)	Low	0x0C(4)	Low
0x10(5)	Low	0x14(6)	Low	0x18(7)	Low	0x1C(8)	Low
0x20(9)	Low	0x24(10)	Low	0x28(11)	Low	0x2C(12)	Low
0x30(13)	Low	0x34(14)	Low	0x38(15)	Low	0x3C(16)	Low
0x40(17)	Normal	0x44(18)	Normal	0x48(19)	Normal	0x4C(20)	Normal
0x50(21)	Normal	0x54(22)	Normal	0x58(23)	Normal	0x5C(24)	Normal
0x60(25)	Normal	0x64(26)	Normal	0x68(27)	Normal	0x6C(28)	Normal
0x70(29)	Normal	0x74(30)	Normal	0x78(31)	Normal	0x7C(32)	Normal
0x80(33)	Medium	0x84(34)	Medium	0x88(35)	Medium	0x8C(36)	Medium
0x90(37)	Medium	0x94(38)	Medium	0x98(39)	Medium	0x9C(40)	Medium
0xA0(41)	Medium	0xA4(42)	Medium	0xA8(43)	Medium	0xAC(44)	Medium
0xB0(45)	Medium	0xB4(46)	Medium	0xB8(47)	Medium	0xBC(48)	Medium
0xC0(49)	High	0xC4(50)	High	0xC8(51)	High	0xCC(52)	High

Activate

設置	说明	出厂设置
Low/Normal/ Medium/High	设置 TOS 值和 4 个输出队列的映射表。	1 to 16: Low 17 to 32: Normal 33 to 48: Medium 49 to 64: High

VLAN 功能

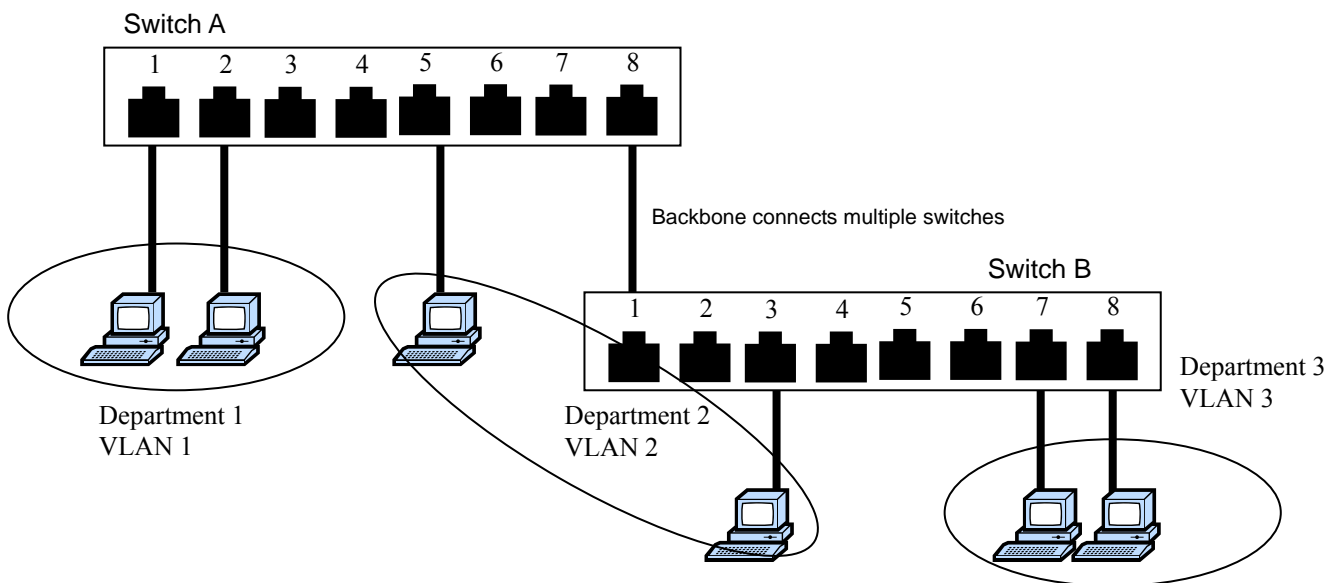
通过将 LAN 分成几个逻辑段（相对物理分段来说），在 EDS-726 上建立虚拟 LAN (VLAN) 来提高网络的效率。通常 VLAN 比 LAN 更容易管理。

VLAN 的概念

什么是 VLAN?

VLAN 是一组可以安放在网络任意位置的一组设备，但是它们之间的通信就象在同一个物理分段中。利用 VLAN 你可以将网络分段而不必受物理连接的限制（传统网络设计的限制）。举个例子来说，你可以按照以下内容对网络进行分段：

- 部门群组一例如，市场部有一个 VLAN，金融部有另一个 VLAN，开发部也有自己的 VLAN。
- 等级群组一例如，总监有一个 VLAN，经理有另一个 VLAN，普通员工也有自己的 VLAN。
- 用途群组一例如，E-mail 用户有一个 VLAN，多媒体用户也有一个 VLAN。



VLAN 的优点

VLAN 的主要优点在于提供了一个网络分段系统，比传统网络具有更高的灵活性。使用 VLAN 还有其他一些优点：

- VLAN 给网络中设备的重新定位带来了方便：在传统网络中，管理员要花大量的时间处理设备的迁移和变化，如果用户转移到一个不同的子网，必须手动升级每个终端的地址。而通过 VLAN 设置，加入市场部 VLAN 的一个终端搬到另一个网络部分的一个端口，

还保留其原来的子网从属关系，只需要在市场部 VLAN 中指明那个新端口，不需要重新布线。

- VLAN 具有更高的安全性能：每个 VLAN 中的设备只能和处在同一个 VLAN 中的设备通信。加入市场部 VLAN 的一台设备要和金融部 VLAN 的设备通信，必须通过第三层交换机的路由设备。
- VLAN 可以帮助控制流量：在传统网络中，阻塞通常是由广播流量引起的，广播信息直接发送到所有设备而不管设备是否需要。VLAN 提高了网络的效率，因为每个 VLAN 只包含相互间需要通信的设备。

VLAN 和 MOXA 以太网交换机

你的 EDS-726 因为使用的 IEEE Std 802.1Q-1998 所以支持 VLAN，IEEE Std 802.1Q-1998 允许多个 VLAN 的流量通过一根物理链接传送，并且允许 EDS-726 上的每个端口对应：

- 任一 EDS-726 定义过的 VLAN
- 几个同时使用 IEEE Std 802.1Q-1998 的 VLAN

IEEE Std 802.1Q-1998 要求在交换机能用 VLAN 转发流量前，必须给 EDS-726 上的每个 VLAN 设置 802.1Q VLAN ID。

VLAN 管理

一个新的或初始化过的 EDS-726 包含一个单独的 VLAN，即默认的 VLAN。这个 VLAN 有以下定义：

- VLAN 名称—VLAN 管理
- 802.1Q VLAN ID—1（如果需要标志的话）

初始化后所有的端口都位于这个 VLAN 中，这是唯一可以通过网络访问 EDS-726 管理软件的 VLAN。

VLAN 之间的通信

如果连接到一个 VLAN 中的设备要和另一个 VLAN 中的设备进行通信，需要安装连接 VLAN 的路由器或者第三层交换设备。只有当 VLAN 都连接到路由器或者第三层交换设备后才能通信。如果连接到一个 VLAN 中的设备要和另一个 VLAN 中的设备进行通信，需要安装连接 VLAN 的路由器或者第三层交换设备。只有当 VLAN 都连接到路由器或者第三层交换设备后才能通信。

VLANs: 标记和未标记的从属关系

EDS-726 支持 802.1Q VLAN 标记，这就使得多个 VLAN 的流量能够在根物理链接（主干）中被传输。在建立 VLAN 的时候你需要了解什么时候使用标记过的或未标记过的 VLAN 的从属关系。很简单，如果一个端口是在一个单独的 VLAN 上，那么这个端口就可以作为未标记的成员，但是假如这个端口是多个 VLAN 的成员，那就需要给这个端口定义从属关系了。

典型的终端（如客户端）将作为 VLAN 的未标记成员，定义为 EDS-726 的访问端口，而交换机之间的连接将作为所有 VLAN 的标记成员，定义为 EDS-726 的 Trunk 端口。

IEEE Std 802.1Q-1998 定义了 VLAN 在开放式分组交换网络中的工作原理。一个 802.1Q 数据包携带额外的信息使得交换机可以决定端口属于哪个 VLAN。如果一个帧携带了额外的信息，这就是有标记的帧。

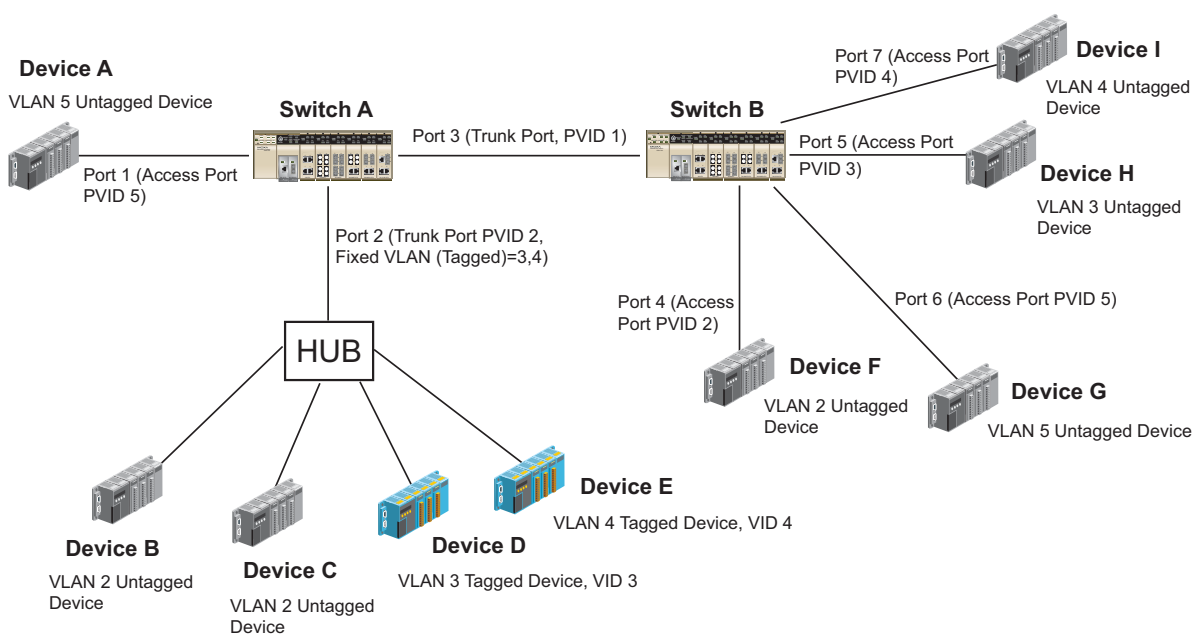
在单个链接（主干）中传输多个 VLAN，每个数据包必须标记一个 VLAN 标志符，那样交换机才能识别数据包属于哪个 VLAN。在 VLAN 之间通信必须使用路由器。

MOXA EDS-726 支持两种 VLAN 端口设置方法，从而方便对标记和未标记的设置：

- 访问端口：连接到单个设备的端口不用做标记。用户必须定义一个默认端口 PVID 来指明设备属于哪个 VLAN。一旦这个访问端口的输入数据包送到另一个 Trunk 端口（该端口需要所有数据包包含标志信息），EDS-726 将在数据包中插入 PVID 来使得下一个 802.1Q 交换机可以识别。
- Trunk 端口：连接到 LAN 的端口包含不带标记设备/带标记设备和/或交换机和 HUB。一般来说，Trunk 端口的流量必须带有标记，用户也可以为 Trunk 端口指定 PVID，Trunk 端口端口的未标记数据包将给端口分配一个默认 PVID 作为它的 VID。

下面描述了如何根据不同的应用使用这些端口。

MOXA EDS-726 VLAN 功能的应用



在这个应用中：

- 端口 1 连接一台单独的未标记设备并将其分配到 VLAN5, 应该设置为访问端口, PVID5。
- 端口 2 将 VLAN2 的两个未标记设备和 LAN 连接起来, 一台设备标记为 VID3 另一台为 VID4. 应该将未标记设备设置为 Trunk 端口, PVID2, 将标记设备设置为固定 VLAN (带标记), 3 和 4. 既然每个端口只能有唯一的 PVID, 同一端口的所有未标记设备只能属于同一个 VLAN。
- 端口 3 连接另一个交换机, 应该设置为 Trunk 端口. 对于 Trunk 端口, 将使用 GVRP 协议。
- 端口 4 连接一台单独的未标记设备并将其分配到 VLAN2, 应该设置为访问端口, PVID2。
- 端口 5 连接一台单独的未标记设备并将其分配到 VLAN3, 应该设置为访问端口, PVID3。
- 端口 6 连接一台单独的未标记设备并将其分配到 VLAN5, 应该设置为访问端口, PVID5。
- 端口 7 连接一台单独的未标记设备并将其分配到 VLAN4, 应该设置为访问端口, PVID4。

在正确设置后:

- 来自设备 A 的数据包将流经 Trunk 端口 3 标记为 VID5, 交换机 B 将识别出它的 VLAN, 将其送到端口 6, 设备 G 将去掉接收到的标志信息, 反之亦然。
- 来自设备 B 和 C 的数据包将流经 Trunk 端口 3 标记为 VID2, 交换机 B 将识别出它的 VLAN, 将其送到端口 4, 设备 F 将去掉接收到的标志信息, 反之亦然。
- 来自设备 D 的数据包将流经 Trunk 端口 3 标记为 VID3, 交换机 B 将识别出它的 VLAN, 将其送到端口 5, 设备 H 将去掉接收到的标志信息。来自设备 H 的数据包将流经 Trunk 端口 3 标记为 PVID3, 交换机 A 将识别出它的 VLAN, 将其送到端口 2, 但是设备 D 无法去掉接收到的标志信息。
- 来自设备 E 的数据包将流经 Trunk 端口 3 标记为 VID4, 交换机 B 将识别出它的 VLAN, 将其送到端口 7, 设备 I 将去掉接收到的标志信息。来自设备 I 的数据包将流经 Trunk 端口 3 标记为 VID4, 交换机 B 将识别出它的 VLAN, 将其送到端口 2, 但是设备 I 无法去掉接收到的标志信息。

配置 802.1Q VLAN

VLAN 端口设置

VLAN Port Setting

Management VLAN ID:

Port	Type	PVID	Fixed VLAN (Tagged)	Forbidden VLAN
1-1	Access	1		
1-2	Access	1		
Trk1	Access	1		

[Activate](#)

要设置 EDS-726 的 VLAN, 进入 VLAN Port Setting 页面来设置端口。

Port Type

設置	说明	出厂设置
Access	该端口类型用来连接单个设备而不需要标记。	Access
Trunk	该端口类型用来连接另一个 802.1Q VLAN 交换机或另一个 LAN, 将标记设备或未标记设备和别的交换机或 HUB 联系起来。	

**注意**

对于 VLAN 环境下的通信冗余，将 Redundant Port、Coupling Port 和 Coupling Control Port 设置为 Trunk Port，因为这些端口必须让所有 VLAN 组的数据包能够通过。

Management VLAN ID

設置	说明	出厂设置
VID 范围从 1 到 4094	设置这台 EDS-726 的 VLAN 管理。	1

Port PVID

設置	说明	出厂设置
VID 范围从 1 到 4094	为连接到端口的未标记设备设置默认端口 VID ID。	1

Port Fixed VLAN List (Tagged)

設置	说明	出厂设置
VID 范围从 1 到 4094	只有当端口类型选择为 Trunk 时该栏才被激活，给连接到 Trunk 端口的标记设备设置其他的 VLAN ID，用逗号区分不同的 VID。	无

Port Forbidden VLAN List

設置	说明	出厂设置
VID 范围从 1 到 4094	只有当端口类型选择为 Trunk 时该栏才被激活，给标记设备设置该 Trunk 端口不支持的 VLAN ID，用逗号区分不同的 VID。	无

VLAN Table

VLAN Table

Management VLAN
Management VLAN 1

Current VLAN List

Index	VID	Joined Access Port	Joined Trunk Port
1	1	1-1, 1-2, Trk1,	

在这张表中你可以查看创建好的 VLAN 组、加入的访问端口以及 Trunk 端口。

注意： 整个物理连接网络系统最多可设置 64 个 VLAN。

Multicast 过滤功能

Multicast 过滤提高了 multicast 网络的性能。本节将介绍 multicast、multicast 过滤以及 EDS-726 是怎么实现 multicast 过滤功能的。

Multicast 过滤的概念

什么是 IP multicast?

Multicast 是一个应用在点对多点以及多点对多点通信中的数据包。用户明确要求通过加入一个终端到一个特殊的 multicast 组来参与通信。如果网络建立无误，一个 multicast 只能传送到一个终端或者一个 LAN 或 VLAN 中的终端的子网，该终端属于相应的 multicast 组，multicast 组成员能分布在多个子网中，因此，multicast 传输能应用在校园 LAN 或者 WAN 中。另外，支持 IP multicast 的网络每次只发送一个期望信息的拷贝，直到发送路径到达组成员的分叉处，只在这个地方，multicast 数据包被复制转发，有效地利用了网络的带宽。multicast 数据包是通过 multicast 组地址来区分的，而 multicast 组地址存在于数据包 IP 报头目的地址中。

Multicast 的优点:

使用 IP multicast 的优点如下:

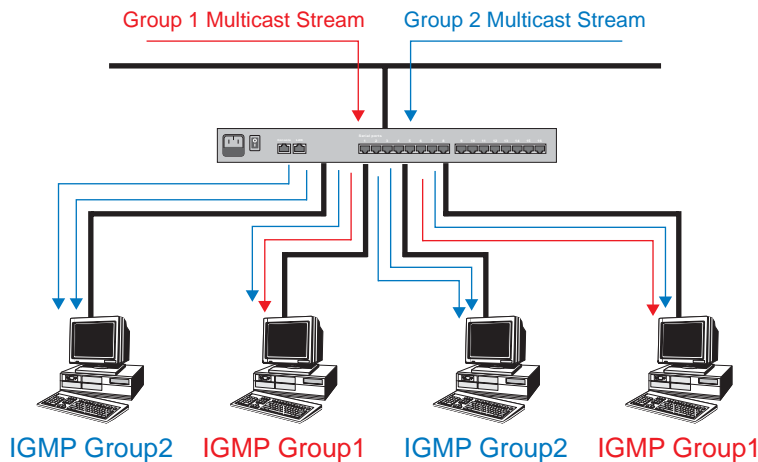
- 能以最高效的逻辑方式向多个接收端传送信息。
- 降低源头（如服务器）的负担，因为不再需要同时产生同一份数据的多个拷贝。
- 能最有效的利用网络带宽以及准确计算 participator 的数量或扩展的协同单元。
- 能和其他 IP 协议以及服务一起工作，如 QoS。

Multicast 有的时候比单播逻辑性更强、效率更高。一个 multicast 的典型应用就是视频会议，需要同时向多个终端传送高质量的语音流量，但是如果用广播方式来传送这些流量的话，将严重降低网络的性能。另外，很多工业自动化协议如 Allen-Bradley、EtherNet/IP、Siemens Profibus 和 Foundation Fieldbus HSE(High Speed Ethernet)都是使用 multicast 方式的。这些工业以太网协议使用的是 publisher/subscriber 通信模型，通过 multicast 数据包将使得大量的数据量充斥整个网络。IGMP Snooping 可以滤除 multicast 流量使得只有那些需要流量的终端才会接收到数据包，从而减少以太 LAN 中的数据流量。

Multicast 过滤

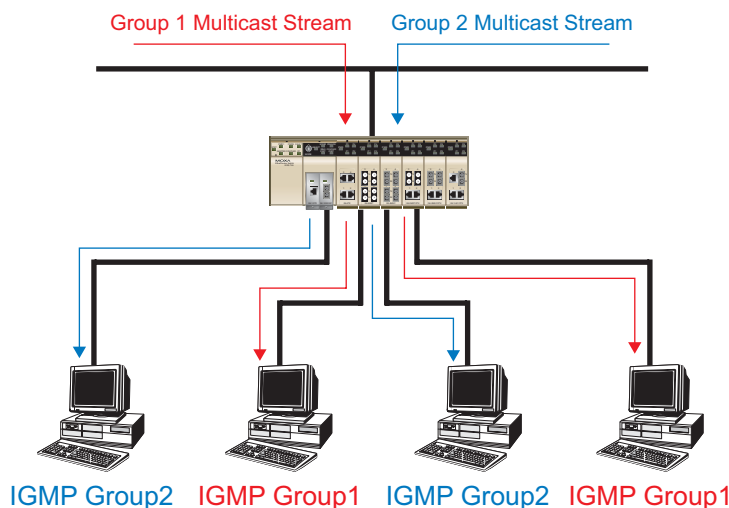
Multicast 过滤保证了只有那些登记加入到特定的 Multicast 组中的终端才能接收到数据，有了 Multicast 过滤功能，网络设备只需要将 multicast 流量转发到连到登记过的终端的端口就行了。从下图可以看到没有 Multicast 过滤功能的网络和有 Multicast 过滤功能的网络的不同之处。

Network without multicast filtering



所有终端必须处理流量不管是否需要。

Network with multicast filtering



终端只接收属于同一个组的指定流量。

Multicast 过滤和 MOXA 以太网交换机

你的 EDS-726 使用 IGMP Snooping 来支持自动 Multicast 过滤功能，它也支持 IGMP 查询模式。

Snooping 模式

在 Snooping 模式下，你的交换机只向合适的端口转发 multicast 流量。交换机探测终端和 IGMP 设备之间的 exchange，最典型的的就是路由器，找出哪些端口要加入到组中，然后相应的设置过滤功能。

查询模式

在查询模式下，如果交换机在所属于网中有最低的 IP 地址，它将作为一个查询器使用。EDS-726 默认开启 IGMP 查询功能，这有助于防止和那些不按照最低 IP 地址选择方式的 multicast 路由器协同工作。如果你想在不包含任何 IGMP 路由器（或查询器）的网络运行 multicast 就启用查询模式。

注意： EDS-726 可以和任何遵守 IGMP v2 以及 IGMP v3 协议的设备兼容。

IGMP Multicast 过滤

IGMP 是所有支持 IP 的网络设备用来在 multicast 组中登记的系统，可以用在包含 multicast IP 路由器的所有 LAN 和 VLAN 中，以及其他支持 multicast 过滤的网络设备中，其工作方式如下：

1. IP 路由器（或查询器）周期性的向连接到 LAN 或 VLAN 的终端发送一个查询数据包，如果你的网络不止一个 IP 路由器，那么 IP 地址最低的那个将作为查询器。如果交换机的 IP 地址比所有连到 LAN 或 VLAN 的 IGMP 查询器的 IP 地址低，那么它将变成 IGMP 查询器。

2. 当 IP 终端接收到查询数据包后，它将发回一个 report 数据包来通知 multicast 组要加入其中。
3. 当 report 数据包到达开启 IGMP Snooping 的交换机端口后，交换机获知该端口将为 multicast 组转发数据，然后将数据包送到路由器。
4. 当路由器接收到 report 数据包后，将为 multicast 组登记 LAN 或 VLAN 需要数据量。
5. 当路由器为 multicast 组转发流量至 LAN 或 VLAN 时，交换机只将流量发送到接收到 report 数据包的端口。

GMRP (GARP Multicast Registration Protocol)

EDS-726 支持 IEEE 802.1D-1998 GMRP (GARP Multicast Registration Protocol)，该协议不同于 IGMP (Internet Group Management Protocol)。GMRP 是基于 MAC 的广播管理协议，而 IGMP 是基于 IP 的广播管理协议。GMRP 允许桥和站动态建立和解除与组之间的成员关系。GMRP 与 GVRP 不同之处在于，GMRP 通过端口来创建 multicast 地址。一旦端口接收到 GMRP-join 消息，在 multicast 地址未被注册的情况下，端口将在自身数据库中创建该 multicast 地址，此时携带 multicast 地址的 multicast 封包便可以通过该端口。若端口接收到一个 GMRP-leave 消息，端口将从自身数据库当中注销该 multicast 地址，所有携带该 multicast 地址的 multicast 封包将被拒绝通过该端口。

静态 Multicast MAC

有一些设备支持广播封包，但不支持 IGMP Snooping 和 GMRP。MOXA EDS-726 支持将 multicast groups 手动添加至 multicast filtering 功能。

启用 Multicast Filtering

您可以通过使用串口 Console 和 Web Console 来启用和禁用 IGMP Snooping 和 IGMP querying。如果禁用 IGMP Snooping，则网络上不在限制 IP multicast 流量，造成网络流量过大。

配置 IGMP Snooping

IGMP Snooping 能够过滤 multicast 流量，那些对终端有用的流量才被传输，因此降低了以太网 LAN 中的流量。

IGMP Snooping 设置

Querier Interval

设置	说明	出厂设置
用户可调数字	设置查询器全局查询的间隔时间，有效时间为 20 到 600 秒	125 秒

IGMP Snooping Enable (Global)

设置	说明	出厂设置
Enable/Disable	检查—标记复选框来开启全局 IGMP Snooping 功能。	Disabled

IGMP Snooping Enable (per VLAN)

设置	说明	出厂设置
Enable/Disable	检查—标记复选框来开启每个 VLAN 的 IGMP Snooping 功能。	如果 IGMP Snooping 功能时全局开启的，那么该项设置就为开启。

Static Multicast Router Port

設置	说明	出厂设置
Select/Deselect	检查—标记复选框来选择哪个端口连接到 multicast 路由器。只有当 IGMP Snooping 开启时才处于激活状态。	Disabled

Querier

設置	说明	出厂设置
Enable/Disable	检查—标记复选框来开启每个 EDS-726 的查询器。	如果 IGMP Snooping 功能时全局开启的，那么该项设置就为开启。

注意： 当同时启用 Turbo Ring 和 IGMP Snooping 时，至少一个交换机必须指定为查询器。

IGMP 表

EDS-726 显示检测到的当前激活的 IGMP。

Current Active IGMP Groups							
VID	Auto Learned Multicast Router Port	Static Multicast Router Port	Querier Connected Port	Act as Querier	Active IGMP Groups		
					IP	MAC	Members Port

信息包含 VID, Auto-learned Multicast Router Port, Static Multicast Router Port, Querier Connected Port, 和激活 IGMP 组的 IP 地址以及 MAC 地址。

加入静态 multicast MAC

MOXA EDS-726 还能手动加入 multicast 组（如果需要的话）。

Add New Static Multicast Address to the List

設置	说明	出厂设置
MAC 地址	输入要加入的 multicast MAC 地址	无

VLAN

設置	说明	出厂设置
Integer	输入主机（具备某一特定 MAC 地址）所属的 VLAN 的数量。	无

Join Port

設置	说明	出厂设置
Select/Deselect	选择该 multicast 组的加入端口	无

配置 GMRP

GMRP 是一项基于 MAC 的广播管理协议，而 IGMP 则基于 IP。GMRP 允许桥和站动态建立和解除与组之间的成员关系。

Port	GMRP	Port Mode
1-1	<input type="checkbox"/> Enable	Forward Unknown
1-2	<input type="checkbox"/> Enable	Forward All
1-3	<input checked="" type="checkbox"/> Enable	Filter Unknown
1-4	<input type="checkbox"/> Enable	Forward Unknown
2-1	<input type="checkbox"/> Enable	Forward Unknown
2-2	<input type="checkbox"/> Enable	Forward Unknown
2-3	<input type="checkbox"/> Enable	Forward Unknown
2-4	<input type="checkbox"/> Enable	Forward Unknown
3-1	<input type="checkbox"/> Enable	Forward Unknown
3-2	<input type="checkbox"/> Enable	Forward Unknown
3-3	<input type="checkbox"/> Enable	Forward Unknown

Activate

Port

設置	说明	出厂设置
x-y	显示启用 GMRP 功能的端口；x-y 是指 x 模块上 y 端口	无

启用 GMRP

設置	说明	出厂设置
Enable/Disable	选择复选框可以启用端口列表中某一端口的 GMRP 功能	禁用

Port Mode

設置	说明	出厂设置
Forward All	在无静态过虑设置 (Add Static Multicast MAC) 的情况下转发所有广播帧	Forward Unknow
Forward Unknown (Unregister)	除两种情况外可以转发所有广播帧：1、有静态过虑设置 (Add Static Multicast MAC)；2、有 Group Registration Entry 过虑设置	Forward Unknow
Filter Unknown (Unregister)	除两种情况外过虑所有广播帧：1、有静态过虑设置 (Add Static Multicast MAC)；2、有 Group Registration Entry 过虑设置	Forward Unknow

GMRP Table

EDS-726 显示当前检测到被激活的 GMRP 组。

GMRP Status			
	Multicast Address	Fixed Ports	Learnt Ports
1	01-01-01-01-01-01	2-1,2-2,	1-3,
2	01-02-02-02-02-02	2-3,2-4,	1-3,
3	01-04-04-04-04-04	3-3,3-4,	1-3,
4	01-03-03-03-03-03	3-1,3-2,	1-3,

設置	说明
Fixed Ports	由静态 multicast 来定义该 multicast 地址
Learnt Ports	由 GMRP 来定义该 multicast 地址

带宽管理

通常来讲是不允许某台主机单独占有网络通信所有带宽的，尤其是在网络设备出现故障的情况下。例如，当网络拓扑配置不当或网络设备故障的时候就有可能导致所谓的“广播风暴”。EDS-726 系列交换机不仅可以防止广播风暴的发生，还可以对所有网络封包设置不同的通过权限，帮助管理员有效地利用有限的带宽，预防意外情况的发生。

配置带宽管理**Broadcast Storm Protection**

Broadcast Storm Protection		
<input checked="" type="checkbox"/> Broadcast Storm Protection <input type="checkbox"/> Include Multicast Packet		
<input type="button" value="Activate"/>		

設置	说明	出厂设置
Enable/Disable	启用或禁用广播风暴保护功能。当网络上有广播和未知封包的时候可能会导致广播风暴。	无
	选择复选框可以在启用广播风暴保护功能的时候接收广播封包。	

Traffic Rate Limiting Settings

Port	Ingress
2-1	Not Limited
2-2	Not Limited
2-3	3%
2-4	5%
	10%
	15%
	25%
	35%
	50%
	65%
	85%

Activate

設置	说明	出厂设置
Ingress rate	从以下选项当中选择所有封包的通过等级: not limited, 3%, 5%, 10%, 15%, 25%, 35%, 50%, 65%, 85%	无

使用端口访问控制

EDS-726 提供了两种基于端口访问控制的方法: IEEE 802.1X 和静态端口锁定 (Static Port Lock)。

IEEE 802.1X

IEEE 802.1X 标准定义了一组基于客户/服务器访问控制和认证的协议。该协议禁止任何未通过认证的客户端借助特定的端口通过 internet 来访问。认证服务器的功能是验证访问该特定端口客户端。只有在得到认证许可的情况下, 客户端才可以访问该端口。

静态端口锁定

EDS-726 可以指定具备某一特定静态 MAC 地址的设备访问指定端口的权限。借助端口锁定功能, 被锁定的端口只接收来自预设静态 MAC 地址设备的数据流而阻止其他任何形式的数据流, 可以有效地防止误操作和阻止黑客的侵入。

IEEE 802.1X 的概念

基于 802.1X 标准的认证机制包含以下三部分内容: 客户端, 认证服务器和认证者。

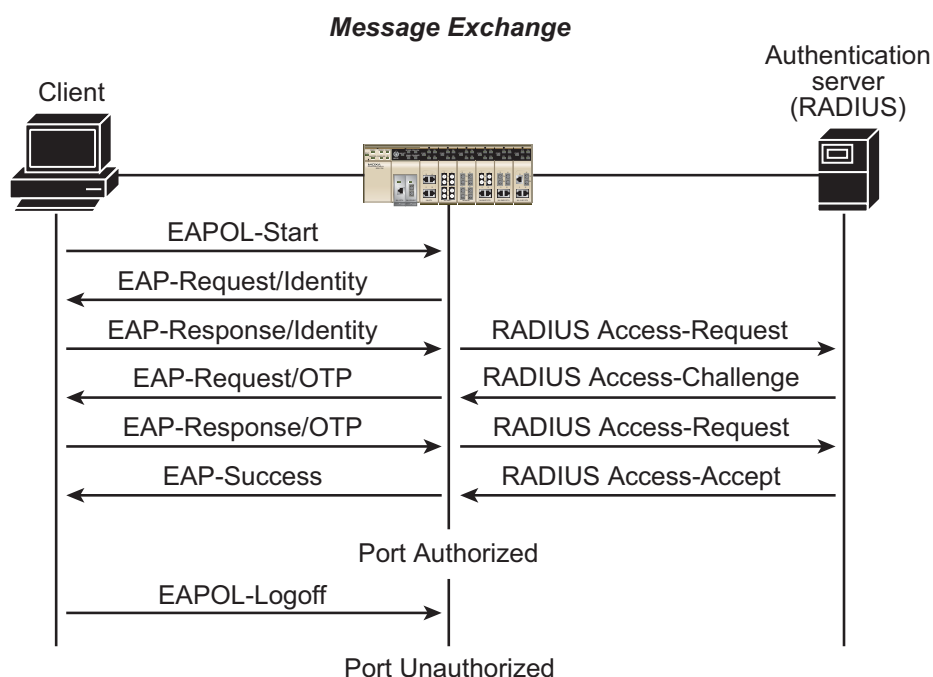
客户端: 是指要求访问 LAN 和交换机的站点, 同时响应来自交换机的请求。

认证服务器: 是指验证来自客户端认证请求的服务器。

认证者: 是指交换机或无线接入点, 它们在客户端和认证服务器之间扮演代理服务器的角色, 包括从客户端获取正确的认证信息然后验证该信息同认证服务器的一致性, 并给客户端相应的回应。

EDS-726 在 802.1X 标准中担任的是认证者的角色。客户端和认证者之间交换的是 EAPOL (Extensible Authentication Protocol over LAN) 帧。我们既可以使用外部 RADIUS 服务器作为认证服务器, 也可以通过使用 Local User Database 作为认证查询表将 EDS-726 作为认证服务器。当我们使用外部 RADIUS 服务器作为认证服务器时, 认证者和认证服务器之间交换的是 EAP 帧。

客户端和认证者均可提出执行认证这一过程。当客户端提出认证时, 它将发送“EAPOL-Start”帧给认证者。而当认证者提出认证或收到“EAPOL Start”帧时, 它将发送“EAP Request/Identity”帧来查询客户端的用户名。如图所示:



1. 当客户端接收到“EAP Request/Identity”帧时, 它会将携带用户名的“EAP Response/Identity”帧发送给认证者。
2. 假如认证服务器为 RADIUS 服务器, 认证者会将来自客户端的“EAP Response/Identity”帧打包成“RADIUS Access-Request”帧的形式发送给 RADIUS 服务器。一旦认证服务器收到该帧, 它便会从自己的数据库当中查询用户名的合法性。若用户名不存在, 则回应的方式有两种情况: a、认证服务器为 RADIUS 服务器时, 认证服务器会向认证者发送“RADIUS Access-Reject”帧; b、当使用的是 Local User Database 时, 直接提示认证者认证失败。接下来, 认证者再将“EAP-Failure”帧发送给客户端。
3. RADIUS 服务器向认证者发送包含“EAP Request” (认证类型) 的“RADIUS Access-Challenge”帧来索取客户端的密码。RFC 2284 定义了各种不同类型的 EAP 认证, 例如: “MD5-Challenge”, “One-Time Password”和“Generic Token Card”。目前被采用的只有“MD5-Challenge”。如果使用的是 Local User Database 方式, 无需考虑认证方式。
4. 认证者将“EAP Request/MD5-Challenge”帧发送给客户端。如果使用的是 RADIUS 服务器, 则“EAP Request/MD5-Challenge”帧的请求将直接从“RADIUS Access-Challenge”帧得到回应。

5. 客户端通过发送 “EAP Response/MD5-Challenge” 的帧（其中包含采用 MD5 hash 算法加密的密码）来响应 “EAP Request/MD5-Challenge” 帧的请求。
6. 假如认证服务器为 RADIUS 服务器，认证者会将来自客户端的 “EAP Request/MD5-Challenge” 帧打包成 “RADIUS Access-Request” 帧的形式发送给 RADIUS 服务器。帧的内容包含有认证者和 RADIUS 服务器中一致的 “共享密钥”。随后 RADIUS 服务器会根据数据库中的信息核对密码，根据核对结果向认证者发送 “RADIUS Access-Accept” 帧或 “RADIUS Access-Reject” 帧。当使用的是 Local User Database 时，密码核对过程将直接通过本地数据库来完成，并向认证者返回认证结果。
7. 认证者根据来自认证服务器的认证信息向客户端发送 “EAP Success” 帧或 “EAP Failure” 帧。

配置 IEEE 802.1X

802.1X Settings

Database Option	<input type="text" value="Local"/>		Re-Auth	<input type="text" value="Enable"/>
Radius Server	<input type="text" value="localhost"/>		Re-Auth Period	<input type="text" value="3600"/>
Server Port	<input type="text" value="1812"/>			
Shared Key	<input type="text"/>			

Port	802.1X
1-3	<input type="checkbox"/> Enable
1-4	<input type="checkbox"/> Enable

802.1X

设置	说明	出厂设置
Enable/Disable	选择位于 802.1X 栏下的复选框可以启用各端口的 IEEE 802.1X。所有用户必须在访问这些端口之前输入正确的用户名和密码。	Disable

Database Option

設置	说明	出厂设置
Local (Max.32 users)	选择此项可将 Local User Database 作为认证服务器的数据库。	Local
Radius	选择此项可将外部 RADIUS 服务器作为认证服务器数据库。其认证机制为“EAP-MD5”。	Local
Radius, Local	选择此项可将外部 RADIUS 服务器作为首选认证服务器数据库，认证机制为“EAP-MD5”。否则采用 Local User Database 作为首选认证数据库。	Local

Radius Server

設置	说明	出厂设置
IP address or domain name	指 RADIUS 服务器的 IP 地址和域名。	Localhost

Server Port

設置	说明	出厂设置
Numerical	RADIUS 服务器的 UDP 端口。	1812

Shared Key

設置	说明	出厂设置
Alphanumeric (Max.40 characters)	是指 RADIUS 服务器和 EDS-726 之间的共享密码。必须设置两者使用相同的密码。	None

Re-Auth Period

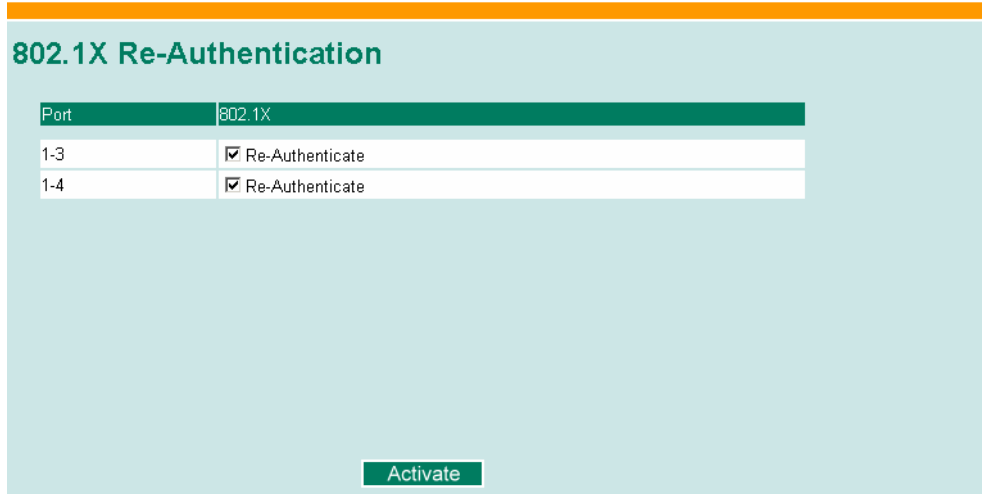
設置	说明	出厂设置
Enable/Disable	在预设时间段内无响应对客户端进行重新认证。	Disable

Re-Auth

設置	说明	出厂设置
Numerical (60-65535sec.)	指定客户端再次输入用户名和密码的频率，保持同认证服务器的连接。	3600 seconds

802.1X Re-Authentication

EDS-726 可以手动选择是否强制所连接的设备执行重新认证的动作。

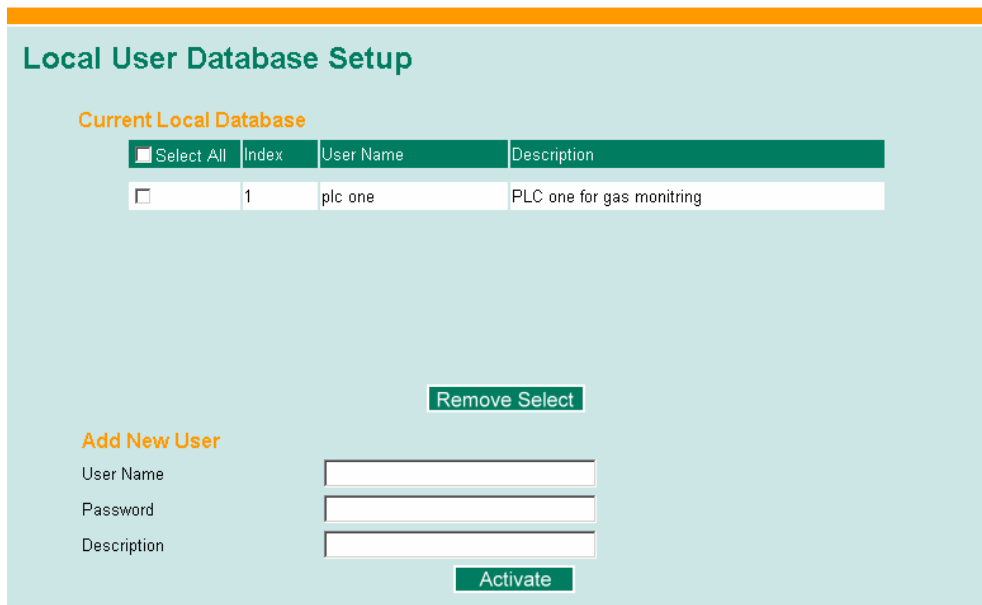


802.1X Re-Authentication

設置	说明	出厂设置
Enable/Disable	选择复选框启用 802.1X Re-Authentication。	Disable

设置 Local User Database

在采用 Local User Database 作为认证数据库之前，请先设置数据库。



Local User Database Setup

設置	说明	出厂设置
User Name (Max. 30 characters)	Local User Database 的用户名	None
Password (Max. 16 characters)	Local User Database 的密码	None
Description (Max. 30 characters)	对 Local User Database 的描述	None

注意: Local User Database 的用户名可根据您的实际需要来命名，比较灵活。

802.1X 表

Port

<input type="checkbox"/> Select All	Index	Mac Address	Status
<input type="checkbox"/>	1	00-04-75-F8-66-6F	Authorized

表中显示了端口是否被授权。

静态端口锁定

MAC Address - - - - -

Port

設置	说明	出厂设置
MAC Address	将静态单播 MAC 地址添加到地址表中。	无
Port	将静态地址绑定到指定端口。	1-1

自动报警功能

工业以太网设备通常位于系统的端点，这些设备无法获知网络其他部分的状态。这就意味着连接这些设备的交换机必须为网络维护人员提供实时的报警信息。甚至当控制工程师离开控制室很长一段时间，当以外发生的时候也能立即知道设备的状态。MOXA EDS-726 支持多种不同的自动报警方式，如 E-mail 和继电器输出。它还支持通过两路数字输入在系统中嵌入传感器来通过自动 E-mail 和继电器输出自动报警。

配置 E-mail 报警

当用户指定的事件发生时，自动 E-mail 报警功能用 E-mail 向用户发出警告。

建立自动报警功能需要以下三个步骤：

1. 配置 E-mail 事件类型
在控制台或 Web 浏览器事件类型页面（关于每个事件的描述，参看 *Email Alarm Events* 部分）中选择需要的事件类型。
2. 配置 E-mail 设置
从控制台接口或浏览器接口配置 EDS-726 E-mail 设置，输入邮件服务器地址/名字（IP 地址或名字），帐户名，帐户密码，重新输入新密码以及要发送到目的邮件地址。
3. 激活你的设置并且如果有必要的话测试 E-mail
在配置并激活 EDS-726 事件类型和 E-mail 设置后，你可以利用 Test E-mail 功能来看你的 E-mail 地址和邮件服务器地址是否设置正确。

E-mail 报警事件设置

Email Alarm Events Settings

System Events

Switch Cold Start
 Switch Warm Start
 Power Transition(On->Off)
 Power Transition(Off->On)
 DI 1(Off)
 DI 1(On)
 DI 2(Off)
 DI 2(On)
 Config. Change
 Auth. Failure
 Comm. Redundancy Topology Changed

Port Events

Port	Link-ON	Link-OFF	Traffic-Overload	Traffic-Threshold(%)	Traffic-Duration(s)
1-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
1-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
1-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
1-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
2-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
2-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
2-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
2-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="1"/>

Event Types

事件类型可以被分为两个基本组：系统事件和端口事件。系统事件涉及交换机的所有功能，而端口事件则是关于特殊端口的活动。

系统事件	当出现以下状况时，发出 Email 警告信息
交换机冷启动	电源被切断，重新连接。
交换机热启动	EDS-726 重新启动，例如网络参数发生改变(IP address, netmask, etc.)
电源转换(On→Off)	EDS-726 断电
电源转换(Off→On)	EDS-726 上电
DI1 (On→Off)	On 到 off 的变化触发数字输入 1
DI1 (Off→On)	Off 到 on 的变化触发数字输入 1
DI2 (On→Off)	On 到 off 的变化触发数字输入 2
DI2 (Off→On)	Off 到 on 的变化触发数字输入 2
激活配置变化	任何配置选项改变
Comm. Redundancy 拓扑改变	任何 Spanning Tree 协议的交换机位置发生改变（只适用于树根）。如果 Turbo Ring 的主机改变或者备用路径被激活。
认证失败	输入密码错误

端口事件	当出现以下状况时，发出 Email 警告信息
链接开	端口连接到另一台设备
链接关	端口连接 断开（如线缆断开或所连接的设备关闭）
流量过载	端口的流量超过门限值（前提是该项功能启用）
流量门限(%)	输入一个非零数字（如果端口的流量过载开启）
流量持续时间(秒)	如果在这个时间内平均流量超过门限，那么将发出一个流量过载警告

注意： 流量过载、流量门限以及流量持续时间是相互关联的。如果你开启了流量过载，那么必须输入一个非零的流量门限百分比值和 1 到 300 之间的流量持续时间值。

注意： Email 警告信息的发送着按照以下格式：

Moxa_EtherDevice_Switch_0001@Switch_Location

其中 **Moxa_EtherDevice_Switch** 是默认的交换机名字，**0001** 是 EDS-726 的序列号，而 **Switch_Location** 是默认的交换机位置。

查看基本设置部分怎样修改交换机的名字和位置。

Email 设置

Mail Server IP/Name

設置	说明	出厂设置
IP 地址	邮件服务器的 IP 地址	无

Account Name

設置	说明	出厂设置
不超过 45 个字符	你的 Email 帐户	无

Password Setting

設置	说明	出厂设置
禁止/允许修改密码	为了能从 Web 浏览器接口重置密码，检查一标记修改密码复选框，输入旧密码、新密码。再输一次新密码，然后执行改变	Disable
旧密码	允许修改密码的情况下，输入当前密码，不超过 45 个字符	无
新密码	允许修改密码的情况下，输入新密码	无
再输一次新密码	如果你在密码栏输入了新密码，在改变密码前还需要在 retype 栏中再输一次新密码	无

Email Address

設置	说明	出厂设置
不超过 30 个字符	你可以设立四个 Email 地址来接收 EDS-726 的警告信息。	无

Send Test Email

在 Email 设置完成后，你首先要点击 **activate** 按钮来执行更改，然后点击 **Send Test Email** 按钮来检查设置是否正确。

注意： 自动Email报警信息将通过一台需要身份认证的SMTP服务器被发送，服务器支持 CRAM-MD5, LOGIN,和 PAIN methods of SASL (Simple Authentication and Security Layer)认证机制。
如果 Email 信息能够不用认证就能发送，我们强烈建议你不要输入帐户名和密码。

配置继电器报警

当用户指定的事件发生时，自动继电器报警功能通过继电器输出 1 向用户发出警告。

建立自动继电器报警功能需要以下三个步骤：

1. 配置继电器 1 事件类型
在控制台或 Web 浏览器事件类型页面（关于每个事件的描述，参看 *Relay Alarm Events* 部分）中选择需要的事件类型。
2. 激活你的设置
在配置完成后激活 EDS-726 继电器事件类型。

继电器报警事件设置

Relay Alarm Events Settings

System Events

Override Relay 1 Warning Settings

Power Input 1 failure(On->Off)

DI 1 (Off) DI 1 (On)

Override Relay 2 Warning Settings

Power Input 2 failure(On->Off)

DI 2 (Off) DI 2 (On)

Port Events

Port	Link	Traffic-Overload	Traffic-Threshold(%)	Traffic-Duration(s)
1-1	<input type="text" value="Ignore"/>	<input type="text" value="Disable"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
1-2	<input type="text" value="Ignore"/>	<input type="text" value="Disable"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
1-3	<input type="text" value="Ignore"/>	<input type="text" value="Disable"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
1-4	<input type="text" value="Ignore"/>	<input type="text" value="Disable"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
2-1	<input type="text" value="Ignore"/>	<input type="text" value="Disable"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
2-2	<input type="text" value="Ignore"/>	<input type="text" value="Disable"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
2-3	<input type="text" value="Ignore"/>	<input type="text" value="Disable"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
2-4	<input type="text" value="Ignore"/>	<input type="text" value="Disable"/>	<input type="text" value="0"/>	<input type="text" value="1"/>

Event Types

事件类型可以被分为两个基本组：系统事件和端口事件。系统事件涉及交换机的所有功能，而端口事件则是关于特殊端口的活动。

MOXA EDS-726 有两路继电器输出，你可以设置哪路输出和哪个事件相关，这有助于管理员识别不同事件的重要性。

系统事件	当出现以下状况时，输出继电器警告信息
电源转换(On→Off)	EDS-726 断电
电源转换(Off→On)	EDS-726 上电
DI1 (On→Off)	On 到 off 的变化触发数字输入 1
DI1 (Off→On)	Off 到 on 的变化触发数字输入 1
DI2 (On→Off)	On 到 off 的变化触发数字输入 2
DI2 (Off→On)	Off 到 on 的变化触发数字输入 2

端口事件	当出现以下状况时，发出 Email 警告信息
链接开	端口连接到另一台设备
链接关	端口连接 断开（如线缆断开或所连接的设备关闭）
流量过载	端口的流量超过门限值（前提是该项功能启用）
流量门限(%)	输入一个非零数字（如果端口的流量过载开启）
流量持续时间(sec.)	如果在这个时间内平均流量超过门限，那么将发出一个流量过载警告

注意： 流量过载、流量门限以及流量持续时间是相互关联的。如果你开启了流量过载，那么必须输入一个非零的流量门限百分比值和 1 到 300 之间的流量持续时间值。

忽略继电器警告设置

检查一标记复选框来临时忽略继电器警告设置，取消继电器输出可以让管理员直到形成报警条件。

继电器报警列表

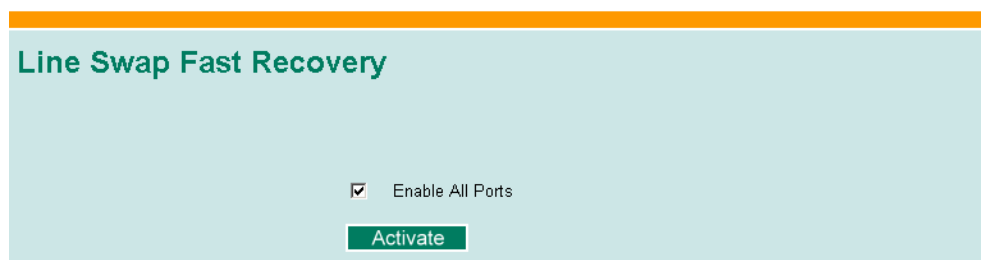
查看此表是否有继电器警告信息发生。

Current Alarm List		
Index	Event	Relay
1	DI 1 failure (Off) !	1
2	DI 2 failure (Off) !	2
3	Port 1-2 Link failure (Off) !	1

Line-Swap-Fast-Recovery 功能

Line-Swap Fast Recovery 功能是默认开启的，可以使 EDS-726 在设备拔出插到另一个端口时迅速恢复正常状态，恢复时间只有几毫秒，而一般商用交换机的恢复时间为几分钟。如果要关闭这项功能或关闭后再重新开启，可以通过控制台组件访问 Line-Swap Recovery 页面或者通过 Web 浏览器接口访问 Line-Swap Fast Recovery 页面，如下所示。

配置 Line-Swap Fast Recovery



Enable Line-Swap-Fast-Recovery

設置	说明	出厂设置
Enable/Disable	检查一标记复选框来开启 Line-Swap Fast Recovery	Enable

Set Device IP 功能

为避免重复设定设备的 IP 地址，EDS-726 系列装有 DHCP/BootP server 和 RARP 协议，可以自动设置以太网设备的 IP 地址。

开启之后，**Set device IP** 功能使得 EDS-726 可以自动给连接的装有 DHCP/BootP client 和 RARP 协议的设备分配特定的 IP 地址。实际上，EDS-726 是作为一个 DHCP/BootP server 给连接设备分配特定的 IP 地址，这些地址保存在 EDS-726 的内存中。每次设备接通或者重新启动，EDS-726 都会向设备发送一个预设的 IP 地址。

按照以下步骤使用 **Set device IP** 功能：

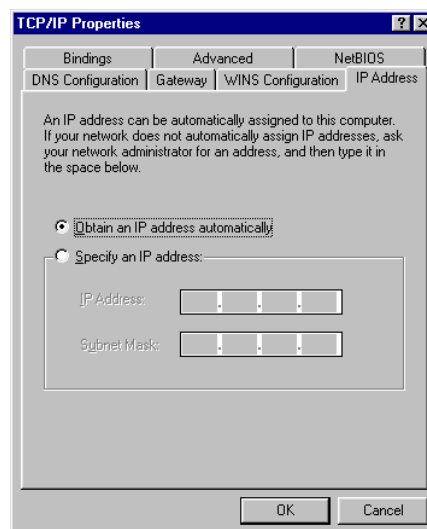
步骤一：建立连接设备

将要自动分配 IP 地址的设备和 EDS-726 建立连接。设备必须设置成自动获取 IP 地址。

设备配置组件必须包含建立页面，那样你就可以和自动获取 IP 地址一样选择其中某个选项。

例如右图是 Windows **TCP/IP Properties** 窗口，也许设备的配置组件看起来有点不同，但是从右图我们可以知道该找什么。

你需要决定你的设备连到 EDS-726 的哪个端口，按照下面的步骤单独建立每个端口。



步骤二:

配置 EDS-726 的 **Set device IP** 功能, 可以通过控制台组件或者 Web 浏览器接口。不管是哪种情况, 你只需简单的为每个需要配置的端口输入预设的 IP 地址。

步骤三:

在退出设置前确定激活你所作的设置。

- 如果是通过 Web 浏览器, 那么只需要点击 **Activate** 按钮来激活设置。
- 如果是通过控制台组件, 首先突出 **Activate** 菜单选项, 然后按回车。你将收到 **the Set device IP settings are now active! (Press any key to continue)** 的信息。

配置 Set Device IP

Port	Device's current IP	Active function	Desired IP address
1-1	NA	--	<input type="text"/>
1-2	NA	--	<input type="text"/>
1-3	NA	--	<input type="text"/>
1-4	NA	--	<input type="text"/>
2-1	NA	--	<input type="text"/>
2-2	NA	--	<input type="text"/>
2-3	NA	--	<input type="text"/>
2-4	NA	--	<input type="text"/>

Activate

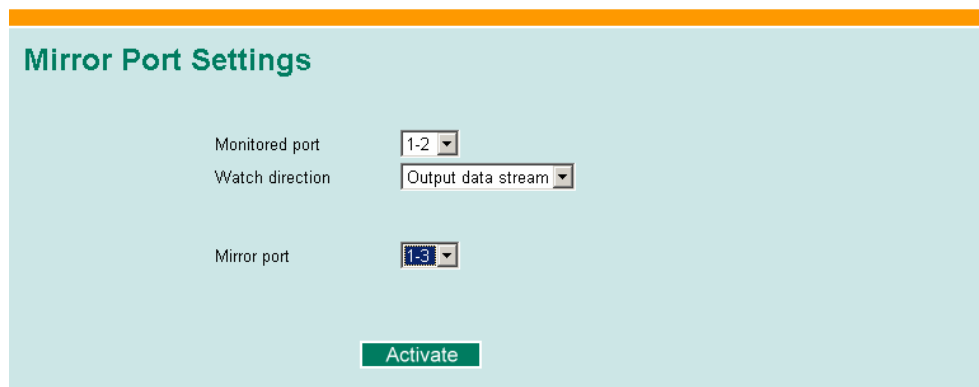
Desired IP Address

設置	说明	出厂设置
IP 地址	为连接设备设定预设的 IP 地址	无

诊断功能

MOXA EDS-726 给管理员提供两种重要的工具来诊断网络系统。

镜像端口



镜像端口功能可以用来监视流过某个特定端口的数据，要做到这一点，需要设定另一个端口（镜像端口）来接收相同的发出或收到的数据来实现的，而我们要做的就是观察那个端口，因此可以掌握网络的动态。

按照以下步骤建立镜像端口功能：

步骤一：

通过控制台组件或 Web 浏览器来配置 EDS-726 的镜像端口功能。你需要配置三项设置：

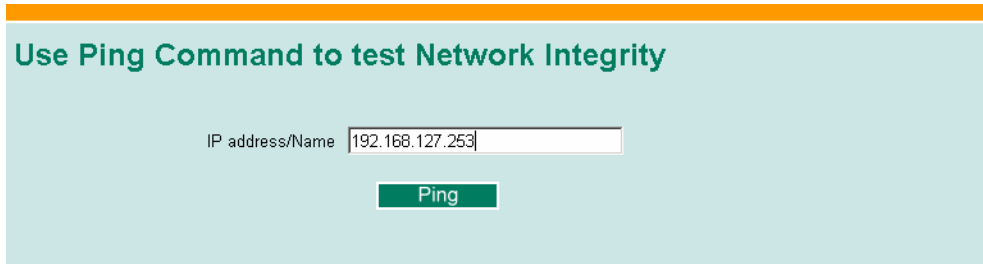
- | | |
|------|---|
| 监视端口 | 选择所要监视网络动态的端口号。 |
| 镜像端口 | 选择一个端口号用来来监视被监视端口的动态。 |
| 观察方向 | 选择以下两个观察方向选项中的一个 <ul style="list-style-type: none">• 输出数据流
选择该选项将只监视通过 EDS-726 端口发送出去的数据包• 双向
选择该选项将监视所有通过 EDS-726 端口流入流出的数据包。 |

步骤二：

在退出设置前确定激活你所作的设置。

- 如果是通过 Web 浏览器，那么只需要点击 **Activate** 按钮来激活设置。
- 如果是通过控制台组件，首先 **highlighting Activate** 菜单选项，然后按回车。你将收到 **the Mirror port settings are now active! (Press any key to continue)** 的信息。

Ping



Ping 功能是使用 Ping 命令提供给用户的简单强大的解决网络问题的工具。该功能最具特色的特点就是尽管命令是在用户 PC 机上输入的，但是实际上命令由 EDS-726 自己发出的，通过这种方法，使得用户可以做到真正意义上的坐在 EDS-726 上通过它的端口发出命令。

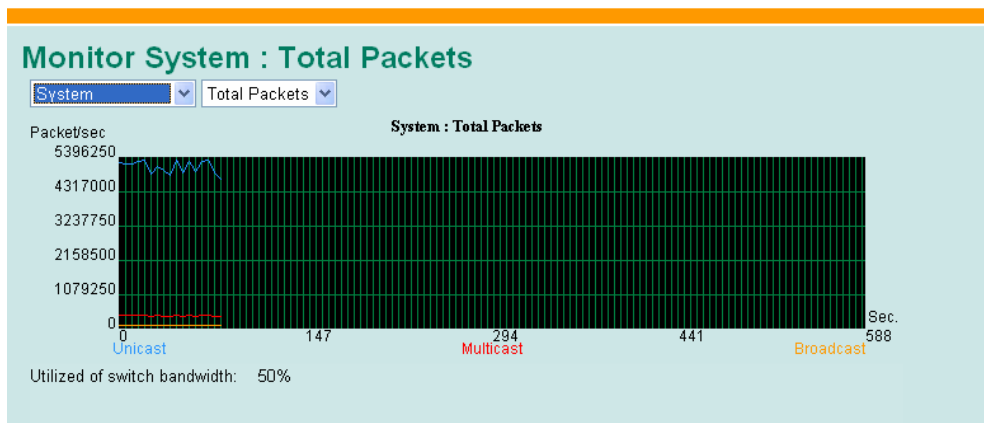
要使用 Ping 功能，输入要操作的 IP 地址，然后在控制台组件下按回车，如果使用的是 Web 浏览器接口，只需要点击 Ping 按钮。

监视器功能

你可以通过 Web 控制台或串口控制台实时监视 EDS-726 的统计数据。

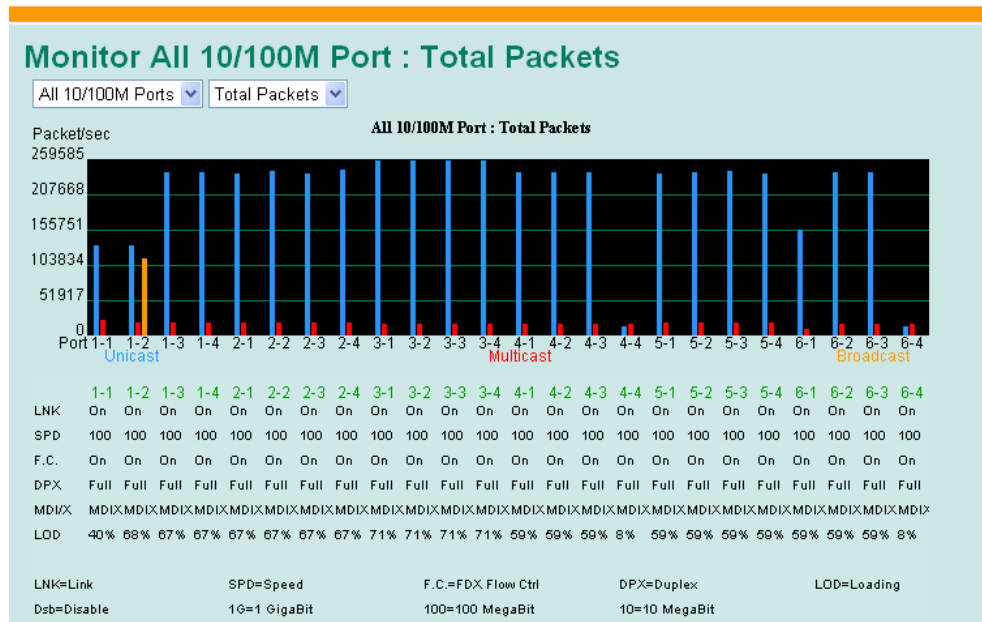
交换机监视

通过选择左边选择栏中的 system 来访问监视器。系统监视下，用户可以看到显示所有 EDS-726 8 个端口数据传输动态的图像。点击四个选项 All Packets, TX Packets, RX Packets, 或 Error Packets 中的一个来观看特定类型数据包的传输动态。回忆一下，TX Packets 是从 EDS-726 发出的，RX Packets 是从连接设备接收的，而 Error Packets 是不通过 TCP/IP 错误检验算法的。All Packets 选项显示的是联合 TX Packets, RX Packets 和 Error Packets 的图像。四幅图(All Packets, TX Packets, RX Packets, 和 Error Packets)的格式是一样的，所以我们这里只显示 All Packets 的图像，它是通过显示每秒多少数据包来描述数据传输动态的。事实上，同一幅图里显示了三种曲线：单播数据包（红色）、组播数据包（绿色）和广播数据包（蓝色）。图像每秒更新一次，这样使得用户可以实时分析数据传输动态。



端口监视

通过端口功能访问监视器，选择左边选择栏中的 **ALL Port/Porti**,其中 $i=1, 2, \dots, 8$ 。Porti 选项和上面谈到的系统监视功能是一致的，那种情况下用户可以看到显示 All Packets, TX Packets, RX Packets,或 Error Packets 动态的图像，而在这种情况下，只能显示某一个单独的端口。**ALL Port** 选项本质上是单个端口动态的图形化显示，可以通过上面提到的控制台监视功能来查看。**ALL Port** 选项给每个端口显示三条垂直线，可以即时查看，线高代表某个数据包类型的速率。也就是说，随着时间的走动，线条的高度也会增高或降低，所以用户可以很直观的看到数据包传输的变化。其中，红色线条代表单播数据包，绿色的代表组播数据包，蓝色的的代表广播数据包。图像每秒更新一次，这样使得用户可以实时分析数据传输动态。



MAC 地址表功能

本部分将介绍 MOXA EDS-726 MAC 地址表。

Index	MAC	Type	VLAN	Port	Priority
1	00-0a-e4-45-f9-1f	ucast()	1	1-1	Low

MAC 地址表可以配置成显示如下 EDS-726 MAC 地址组：

ALL	显示所有 EDS-726 MAC 地址
ALL Learned	显示所有 EDS-726 Learned MAC 地址
ALL Static Lock	显示所有 EDS-726 Static Lock MAC 地址
ALL Static	显示所有 EDS-726 Static/Static Lock /Static Multicast MAC 地址
ALL Static Multicast	显示所有 EDS-726 Static Multicast MAC 地址
Port x	显示所有 EDS-726 指定端口的 MAC 地址

MAC 地址表中显示的是以下信息：

MAC	本栏显示的是 MAC 地址
Type	本栏显示的是 MAC 地址的类型
Port	本栏显示的是 MAC 地址从属于的端口
Priority	本栏显示的是 MAC 地址的优先级

事件日志功能

Event Log Table

Page 2/2

Index	Bootup	Date	Time	System Startup Time	Event
16	3	1970-01-01	00:00:06	0d0h0m6s	Port 1-1 link off
17	3	1970-01-01	00:00:07	0d0h0m7s	Port 1-1 link on
18	3	1970-01-01	04:07:27	0d4h7m27s	Configuration change activated
19	3	1970-01-01	04:17:54	0d4h17m54s	Configuration change activated
20	4	1970-01-01	00:00:06	0d0h0m6s	Cold start
21	4	1970-01-01	00:00:06	0d0h0m6s	Port 1-1 link off
22	4	1970-01-01	00:00:06	0d0h0m6s	Port 1-1 link on

Clear

事件表中显示以下信息

Bootup	本栏显示 EDS-726 重启或冷启动的次数
Date	该日期将根据基本设置页中设定的当前日期更新
Time	该日期将根据基本设置页中设定的当前时间更新
System Startup Time	和该事件相关的系统启动时间
Events	已发生的事件

EDS 配置器图形用户界面

EDS 配置器是易理解的基于 Windows 的图形用户界面，它可以用来配置和维护多个 EDS-726 交换机。该工具有助于您定位同一 LAN 中作为类似 PC 主机（不管是否知道交换机的 IP 地址）的 EDS-726，连接已知 IP 地址的 EDS-726，修改一个或多个 EDS-726 的网络配置，以及升级一个或多个 EDS-726 的固件。EDS 配置器是针对实时控制所有 EDS-726 设计的，可以不用考虑具体交换机位的位置。您可以从 MOXA 公司的网站上免费下载 EDS 配置器软件。

本章包括以下内容：

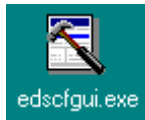
- 启动 EDS 配置器
- 广播搜索
- 通过 IP 地址搜索
- 升级固件
- 修改 IP 地址
- 导出配置文件
- 导入配置文件
- 解除服务器的锁定

启动 EDS 配置器

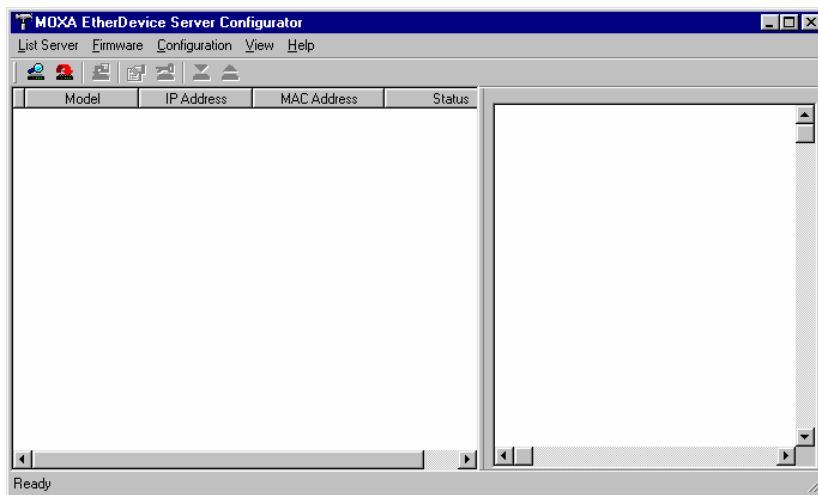
要启动 EDS-726 配置器，先找到 **edscfgui.exe** 文件然后运行。

注意： 你可以从 MOXA 公司的网站 www.moxa.com 上下载 EDS-726 配置器软件。


举例来说，如果文件位于 Windows 桌面上，如下图所示，直接双击图标就可以运行程序了。



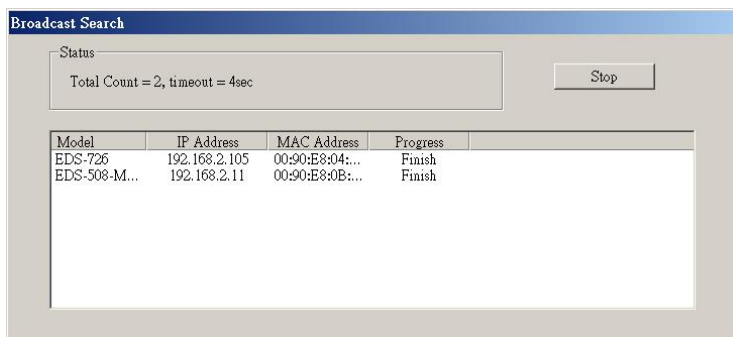
MOXA EDS 配置器打开后，如下图所示。



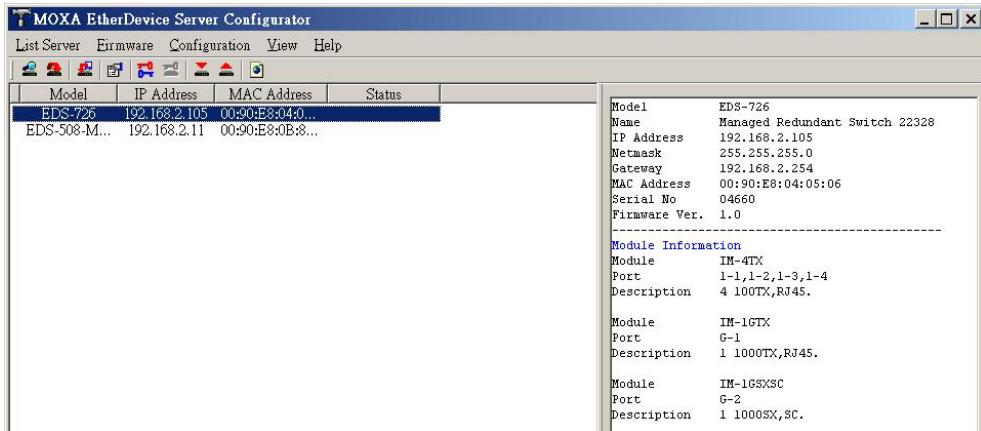
广播搜索

使用广播搜索组件来搜索连接到 LAN 中的 EDS-726，要注意的是，既然搜索是通过 MAC 地址来实现的，所以广播搜索不能定位不在 PC 主机相同 LAN 中的 MOXA EDS-726 服务器。点击广播搜索图标  或者选择 List Server 菜单栏下面的 Broadcast Search 开始搜索。

广播搜索窗口将打开，在搜索的过程中显示位于网络中的所有交换机。



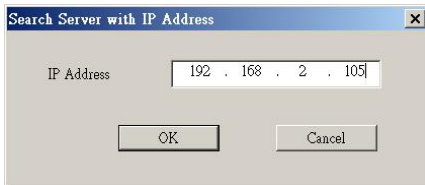
一旦搜索完成后，配置器窗口将显示所有找到的交换机。



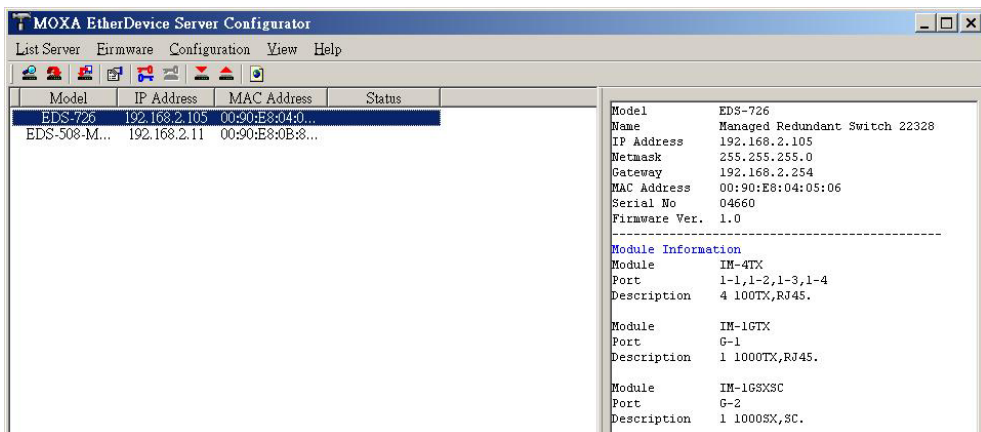
通过 IP 地址搜索

该功能用来每次只搜索一台 EDS-726。注意到搜索是通过 IP 地址来实现的，所以你能够找到任何 EDS-726，只要它准确连接到 LAN、WAN 或者 Internet。点击指定 IP 地址图标  或者选择 List Server 菜单栏下面的 **Specify IP address** 开始搜索。

通过 IP 地址搜索服务器窗口将打开，输入你要查找的 IP 地址，然后点击 **OK**。



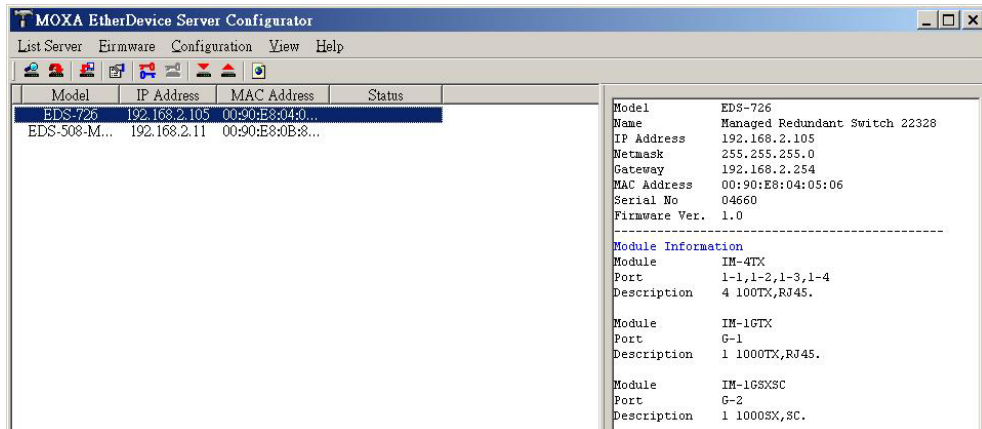
一旦搜索完成后，配置器窗口将把搜索到的交换机加入到交换机列表中。




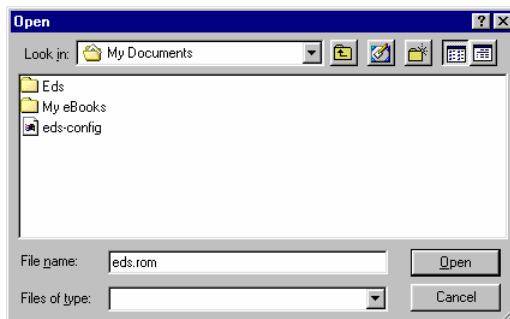
升级固件

根据 MOXA 公司最新的固件随时更新你的 MOXA EDS-726。按照以下步骤来升级 EDS-726 固件：

1. 从 MOXA 公司网站上下载最新的固件文件 (*.rom)。
2. 选择你想升级固件的交换机（在配置器窗口下）。



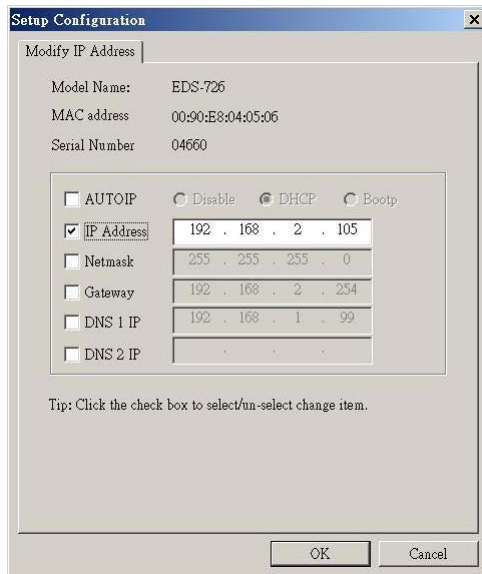
3. 点击升级固件图标  或者选择 **Firmware** 菜单栏下面的 **Upgrade** 来进行升级。如果交换机被锁住了，你将被提示输入交换机的用户名和密码。
4. 使用 **Open** 窗口查找包含固件升级文件的文件夹，然后点击选择正确的*.rom（见下图例子中的 eds.rom），点击 **Open** 来激活升级程序。



修改 IP 地址

你可以使用修改 IP 地址功能来重新配置 EDS-726 的网络设置。点击修改 IP 地址图标或者选择 **Configuration** 菜单栏下面的 **Modify IPaddress** 开始。

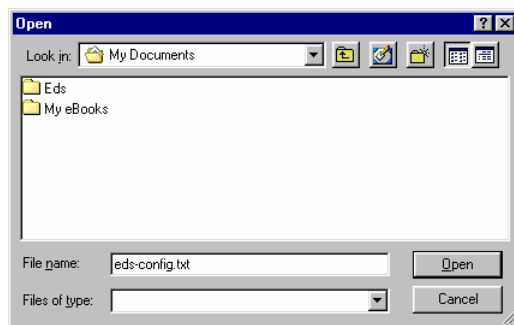
Setup Configuration 窗口将打开，将要修改选项左边得复选框钩上，然后关闭或开启 DHCP，输入 IP 地址，子网掩码，网关以及 DNS IP。点击 OK 执行更改。



导出配置文件

导出配置内容功能用来将特殊交换机的配置保存为文本文件。按照以下步骤导出配置文件：

1. 选择交换机（从配置器窗口左边的服务器列表中选择），然后点击导出图标或者选择 **Configuration** 菜单栏下面的 **Export Configuration**，打开窗口选择要保存文件的文件夹，然后在文件名输入框下输入要保存文件的文件名，点击 **Open**。



2. 当 **Export configuration to file OK** 信息弹出时点击 **OK**。



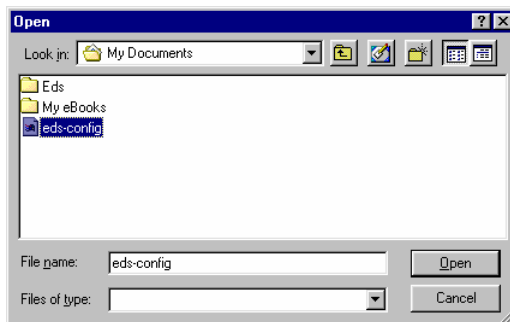
3. 你可以使用标准的文本编辑器，如 Windows 下面的 Notepad 来查看或修改新创建的配置文件。

```
[EtherDevice Server Configuration File]
# Model Name
modelName                EDS-726
#####
# System Identification
#####
# [SwitchName]: Switch Name
# --> max. length = 30 words
SwitchName                Managed Redundant Switch 22328
# [Location]: Switch Location
# --> max. length = 80 words
Location                  Switch Location
# [SysDescr]: Switch Description
# --> max. length = 30 words
SysDescr
# [Contact]: Maintainer Contact Info
# --> max. length = 30 words
Contact
# [WebConfig]: Web Configuration
# --> 0 : Disable Web Configuration
```

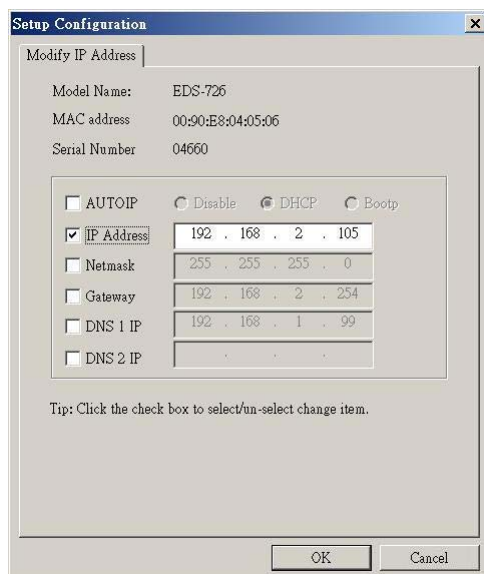
导入配置文件

导入配置文件功能是将文本文件中的整个配置文件导入到 EDS-726 中，该功能可以用来将一个交换机的配置文件转移到另一个交换机，首先利用配置文件导出功能（见上一部分）导出配置文件，然后再使用导入功能。按照以下步骤导入配置文件：

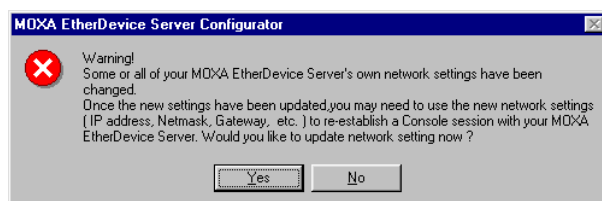
1. 选择交换机（从配置器窗口左边的交换机列表中选择），然后点击导入图标  或者选择 **Configuration** 菜单栏下面的 **Import Configuration**。
2. 使用 **Open** 窗口查找包含配置文件的文本文件，一旦文件选定后，点击 **Open** 初始化导入过程。



3. 出现 **Setup Configuration** 窗口在窗口底部有一段特殊提示。可修改的参数前面的复选框将是选中状态，如果有必要的话，你可以修改其中的参数，然后点击 OK 执行更改。



4. 在出现的警告信息上点击 YES 接受新的设置。




解除服务器的锁定

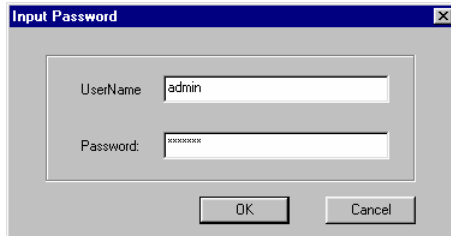
解除服务器锁定功能用来打开一个受密码保护的交换机，那样用户就可以修改它的配置，导入/导出配置文件，等等。在开始之前，先指出在状态栏中有 6 个可能的响应。EDS-726 的状态显示了交换机是怎么安置的（通过 EDS-726 配置器），有什么样的密码保护类型。

6 个选项如下所示（注意：术语 Fixed 来源于标准的网络术语 Fixed IP Address）：

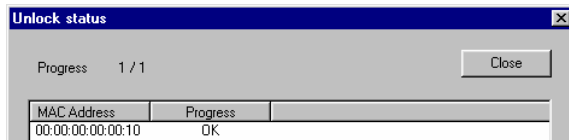
- **Locked**
交换机受密码保护，使用广播搜索来定位交换机，在当前配置中没有输入密码。
- **Unlocked**
交换机受密码保护，使用广播搜索来定位交换机，在当前配置中已经输入密码。以后在配置过程中激活交换机的各项功能不需要再输入服务器密码。
- **Blank**
交换机不受密码保护，使用广播搜索来定位交换机。
- **Fixed**
交换机不受密码保护，通过 IP 地址搜索来手动定位交换机。
- **Locked Fixed**
交换机受密码保护，通过 IP 地址搜索来手动定位交换机，在当前配置中没有输入密码。
- **Unlocked Fixed**
交换机受密码保护，通过 IP 地址搜索来手动定位交换机，在当前配置中已经输入密码。以后在配置过程中激活交换机的各项功能不需要再输入服务器密码。

按照以下步骤来开启一台被锁定 EDS-726（EDS-726 的状态为 Locked 或 Locked Fixed），选择交换机（从配置器窗口左边的交换机列表中选择），然后点击解锁图标  或者选择 **Configuration** 菜单栏下面的 **Unlock**。

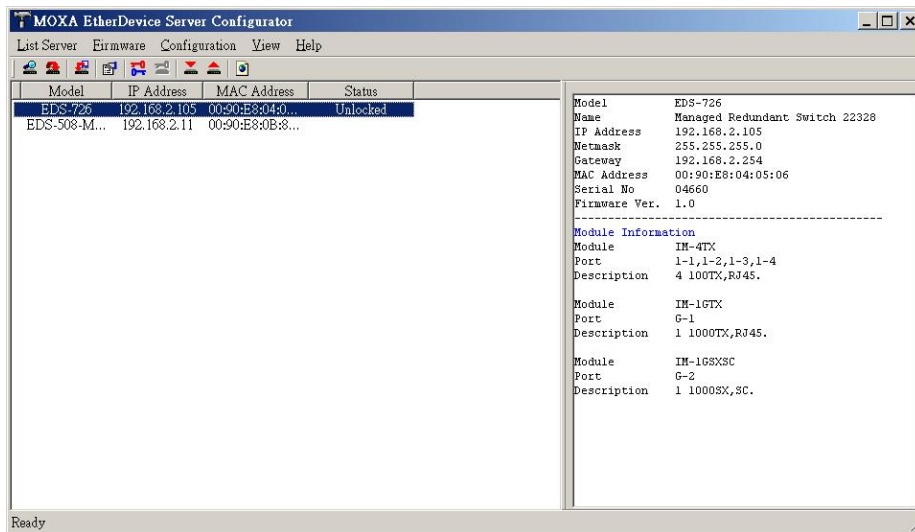
1. 按照提示输入交换机的用户名和密码，然后点 OK。



2. 当解锁窗口报告解锁过程 OK，点击窗口右上角的 Close。



3. 交换机的状态将为 Unlocked 或 Unlocked Fixed。



A

MIB 组

MOXA EDS-726 随机带有内建的 SNMP (Simple Network Management Protocol)代理软件, 支持冷/热启动 trap, line up/down trap,以及 RFC 1213 MIB-II。

MOXA EDS-726 系列支持以下标准的 MIB 组:

MIB II.1 – System Group

sysORTable

MIB II.2 – Interfaces Group

ifTable

MIB II.4 – IP Group

ipAddrTable

ipNetToMediaTable

IpGroup

IpBasicStatsGroup

IpStatsGroup

MIB II.5 – ICMP Group

IcmpGroup

IcmpInputStatus

IcmpOutputStats

MIB II.6 – TCP Group

tcpConnTable

TcpGroup

TcpStats

MIB II.7 – UDP Group

udpTable

UdpStats

MIB II.10 – Transmission Group

dot3
dot3StatsTable

MIB II.11 – SNMP Group

SnmpBasicGroup
SnmpInputStats
SnmpOutputStats

MIB II.17 – dot1dBridge Group

dot1dBase
 dot1dBasePortTable
dot1dStp
 dot1dStpPortTable
dot1dTp
 dot1dTpFdbTable
 dot1dTpPortTable
 dot1dTpHCPortTable
 dot1dTpPortOverflowTable
pBridgeMIB
 dot1dExtBase
 dot1dPriority
 dot1dGarp
qBridgeMIB
 dot1qBase
 dot1qTp
 dot1qFdbTable
 dot1qTpPortTable
 dot1qTpGroupTable
 dot1qForwardUnregisteredTable
dot1qStatic
 dot1qStaticUnicastTable
 dot1qStaticMulticastTable
dot1qVlan
 dot1qVlanCurrentTable
 dot1qVlanStaticTable
 dot1qPortVlanTable

EDS-726 还提供私有 MIB 文件，位于光盘的 MOXA-EDS726-MIB.my 文件中。

Public Traps:

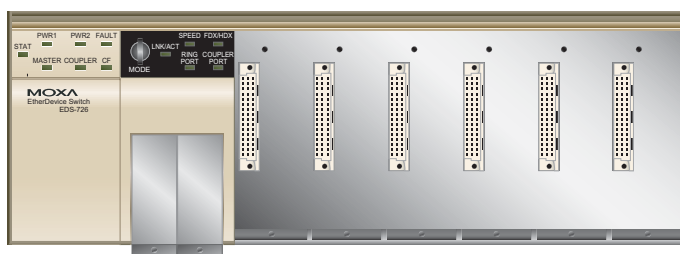
1. Cold Start
2. Link Up
3. Link Down
4. Authentication Failure
5. dot1dBridge New Root
6. dot1dBridge Topology Changed

Private Traps:

1. Configuration Changed
2. Power On
3. Power Off
4. Traffic Overloaded
5. Turbo Ring Topology Changed
6. Turbo Ring Coupling Port Changed
7. Turbo Ring Master Mismatch
8. CF Save
9. CF Load
10. Module Inserted
11. Module Removed

网管型、模块化交换机系统，EDS-72610G

具备 6 个插槽的模块化、网管型交换机，最多可以扩展只 26 个端口。



技术参数

标准	IEEE802.3, 802.3u, 802.3x, 802.1D, 802.1w, 802.1Q, 802.1p, 802.1X, 802.3ad, 802.3z
协议	IGMP Snooping, GMRP, GVRP, SNMP V1/V2C/V3, DHCP Server/Client, BOOTP, TFTP, SNTP, SMTP, RARP, RMON and EDS-SNMP OPC Server Pro (Optional)
MIB	MIB-II, Ethernet-Like MIB, P-BRIDGE MIB, Q-BRIDGE MIB, Bridge MIB, RSTP MIB, RMON MIB Groups 1, 2, 3, 9 (即将推出)
流控	IEEE802.3x flow control/back pressure

接口

快速以太网	6 个插槽可安装任意 4 端口 10/100M 或者 100MFX 的接口模块
千兆以太网	2 个插槽可安装任意 1 端口 10/100/1000BaseT (X), 1000BaseSX, 1000BaseLX, 1000BaseLHX 或者 1000Base ZX 的接口模块
闪存接口	提供
Console	RS-232 (RJ45)
系统 LED 指示灯	STAT, PWR1, PWR2, FAULT, MASTER, COUPLER, CF
模块 LED 指示灯	LNK/ACT, FDX/HDX, RING PROT, COUPLER PORT, SPEED
报警输出	两个输出能力为 1A@24VDC 的继电器电流输出
数字输入	共地，隔离； <ul style="list-style-type: none">• 状态 "1": +13 到 +30V• 状态 "0": -30 到 +3V• 最大输入电流: 8 mA

电源

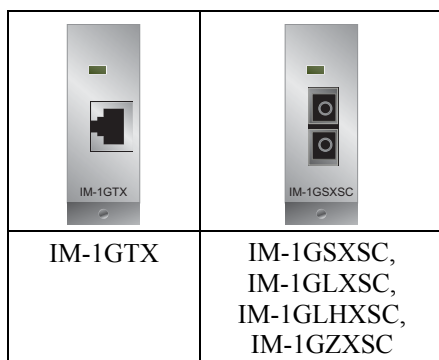
输入电压	24 VDC (12—45 VDC), 冗余双电源输入	
连接形式	两组可拆卸 6 脚接线端子	
电源功耗	EDS-72610G	21.5W
	IM-4TX	2.5W
	IM-2MSC/2TX	5W
	M-2MST/2TX	5W
	IM-2SSC/2TX	5W
	IM-4MSC	7.2W
	IM-4MST	7.2W
	IM-4SSC	7.2W
	IM-1LSC/3TX	4W
	IM-1GTX	2.5W
	IM-1GSXSC	1.5W
	IM-1GLXSC	1.5W
	IM-1GLHXSC	1.5W
	IM-1GZXSC	1.5W
过流保护	提供	
反向保护	提供	

机械规格

外壳	IP30 等级保护
尺寸	362 × 146 × 128 mm (W x H x D)
安装方式	导轨, 壁挂式 (可选组件)

千兆以太网接口模块, IM 系列

IM-1GTX:	1 个 10/100/1000BaseT(X)端口, RJ45 接口的接口模块
IM-1GSXSC:	1 个 1000BaseSX 端口, SC 接口的接口模块
IM-1GLXSC:	1 个 1000BaseLX 端口, SC 接口的接口模块
IM-1GLHXSC:	1 个 1000BaseLHX 端口, SC 接口的接口模块, 40 km
IM-1GZXSC:	1 个 1000BaseZX 端口, SC 接口的接口模块, 80 km



界面

LED 指示灯	端口状态
RJ45 端口	10/100/1000BaseT (X) 速度自适应, 带自动 MDI/MDI-X 连接功能
距离	100m
光口	100BaseSX/LX/LHX/ZX (SC 接头)

光纤

距离

多模

IM-1GSXSC	0 to 500 m, 850 nm (50/125 μ m, 400 MHz*km)
IM-1GLXSC	0 to 275 m, 850 nm (62.5/125 μ m, 200 MHz*km)
IM-1GLXSC	0 to 1100 m, 1310 nm (50/125 μ m, 800 MHz*km)
IM-1GLXSC	0 to 550 m, 1310 nm (62.5/125 μ m, 500 MHz*km)

单模

IM-1GLXSC	0 to 10 km, 1310 nm (9/125 μ m, 3.5 PS/(nm*km))
IM-1GLHXSC	0 to 40 km, 1310 nm (9/125 μ m, 19 PS/(nm*km)) TBD
IM-1GZXSC	0 to 80 km, 1550 nm (9/125 μ m, 19 PS/(nm*km)) TBD

最小 TX 输出

1M-GSX	-9.5 dB
1M-1GLX	-9.5 dB
1M-1GLHX	-4 dB
1M-1GZX	0 dB

最大 TX 输出

1M-GSX	-4 dB
1M-1GLX	-3 dB
1M-1GLHX	+3 dB
1M-1GZX	+5 dB

灵敏度

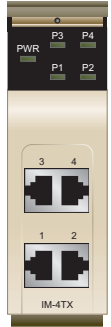

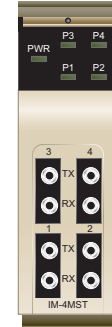



1M-GSX	0 to -18 dB
1M-1GLX	-3 to -20 dB
1M-1GLHX	-3 to -23 dB
1M-1GZX	-3 to -23 dB

机械规格

尺寸	24 x 66 x 101 mm (W x H x D)
----	------------------------------

快速以太网接口模块，IM 系列

- IM-4TX:** 4个10/100BaseT(X) 端口, RJ45接口的接口模块
- IM-4MSC:** 4个多模100BaseFX端口, SC接口的接口模块
- IM-4MST:** 4个多模100BaseFX端口, ST接口的接口模块
- IM-4SSC:** 4个单模100BaseFX端口, SC接口的接口模块, 40 km.
- IM-2MSC/2TX:** 2个多模100BaseFX端口,SC接口; 2个10/100BaseT(X)端口,RJ45接口的接口模块
- IM-2MST/2TX:** 2个多模100BaseFX端口,ST接口; 2个10/100BaseT(X) 端口,RJ45接口的接口模块
- IM-2SSC/2TX:** 2个单模100BaseFX端口,40km,SC接口; 2个10/100BaseT(X)端口, RJ45接口的接口模块
- IM-1LSC/3TX:** 1个单模100BaseFX端口,80km,SC接口; 3个10/100BaseT(X) 端口, RJ45接口的接口模块

					
IM-4TX	IM-4MSC, IM-4SSC,	IM-4MST	IM-2MSC/ 2TX IM-2SSC/ 2TX	IM-2MST/ 2TX	IM-1LSC/ 3TX

界面

LED 指示灯	PWR,P1,P2,P3,P4 端口状态
RJ45 端口	10/100/1000BaseT (X) 速度自适应, 全/半双工模式, 带自动连接 MDI/MD-X 功能
距离	100m
光口	100BaseFX 端口 (SC/ST 接口)

光纤

距离	
多模	IM-4MSC, IM-4MST, IM-2MSC/2TX, IM-2MST/2TX 0 to 5 km, 1310 nm (50/125 μ m, 800 MHz*km) 0 to 4 km, 1310 nm (62.5/125 μ m, 500 MHz*km)
单模	IM-4SSC 0 to 40 km, 1310 nm (9/125 μ m, 3.5 PS/(nm*km)) IM-1LSC/3TX 0 to 80 km, 1550 nm (9/125 μ m, 19 PS/(nm*km))

最小 TX 输出	
多模	-20 dBm
单模	0 to 40 km, -5 dBm 0 to 80 km, -5 dBm
最大 TX 输出	
多模	-14 dBm
单模	0 to 40 km, 0 dBm 0 to 80 km, 0 dBm
灵敏度	
多模	-34 to -30 dBm
单模	-36 to -32 dBm
机械规格	
外壳	IP30 防护等级
尺寸	24 x 66 x 101 mm (W x H x D)
环境	
操作温度	0 到 60°C (32 到 140°F)
存储温度	-40 到 85°C (-40 到 185°F)
周围环境相对湿度	5%到 95% (无凝露)
安规认证	
安全	UL60950 (E212360), UL 508, CSA C22.2 No. 60950, EN60950 (E212360) (Pending)
危险区域	UL/cUL Class I, Division 2, Groups A, B, C and D (Pending) ATEX Class I, Zone 2, EEx nC IIC (Pending)
EMI	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD), Level 3 EN61000-4-3 (RS), Level 3 EN61000-4-4 (EFT), Level 3 EN61000-4-5 (Surge), Level 3 EN61000-4-6 (CS), Level 3 EN61000-4-8 EN61000-4-11 EN61000-4-12
冲击	IEC60068-2-27
自由下落	IEC60068-2-32
震动	IEC60068-2-6
保修期	5 年

C

服务信息

本章将介绍如何关于本产品或其他产品和 MOXA 联系，以及如何报告您的问题。

包括以下内容。

- MOXA Internet 服务**
- 故障报告单**
- 返修流程**

MOXA Internet 服务

让客户满意是我们的宗旨, 因此为了确保客户的最大利益, MOXA 公司设立了 Internet 服务, 提供技术支持, 驱动更新, 产品信息, 以及用户手册更新等。

提供以下服务

技术支持E-mail support@moxanet.com

产品信息网址 <http://www.moxa.com>

故障报告单

MOXA EDS-726 Series

用户姓名:	
公司:	
电话号码:	传真号码:
E-mail:	日期:

Serial Number: _____

问题描述: 请尽可能清楚详细的描述你所遇到的问题，包括你看见的错误信息。我们将根据你的描述再现这些问题，所以请将你遇到的问题完整的描述出来。

返修流程

要进行产品维修、调换，必须提供：

- ◆ 产品原始购买凭证或正式发票。
- ◆ 从经销商处取得产品返修单。
- ◆ 尽可能详细填写返修单，那样我们可以尽快修复产品。
- ◆ 使用防静电的包装袋认真包装待修产品，返修单应放在包装明显处，填写好返回地址以及电话联系方式后寄出。