讲解系统网络知识

介绍管理维护技能

提供专业网管经验

荟萃网络使用技巧

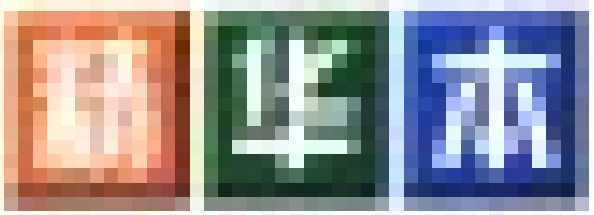
《网管员世界》杂志社　编

《网管员世界》

精华本

机械工业出版社
CHINA MACHINE PRESS

《网管员世界》



《网管员世界》精华本

《网管员世界》杂志社　编

机械工业出版社

本书集中了《网管员世界》自创刊以来受到网管员朋友欢迎的众多实用性文章，便于读者收藏保管及查找资料。本书内容涵盖了网络管理的方方面面，全书分网络设备、Windows 系统维护及应用、Linux 系统维护与应用、数据库、网络安全 5 篇。同时，考虑到一些读者的需求，新增了附录“ADSL 全攻略”的专题内容。

本书可作为网管员的工作手册，在工作中遇到问题时随时查找；或作为一般网管员充实提高的进阶工具，在工作之余进行研习。本书也可作为广大网络爱好者和其他网络从业人员探索网络技术的工具书或参考资料。

图书在版编目（CIP）数据

《网管员世界》精华本 /《网管员世界》杂志社编.—北京：机械工业出版社，2004.6
ISBN 7-111-14421-X

Ⅰ.网…Ⅱ.网…　Ⅲ.计算机网络－基本知识　Ⅳ.TP393

中国版本图书馆 CIP 数据核字（2004）第 040742 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）
策　　划：胡毓坚
责任编辑：车　忱
责任印制：李　妍

北京蓝海印刷有限公司印刷 • 新华书店北京发行所发行

2004 年 6 月第 1 版 • 第 1 次印刷

787mm×1092mm 1/16 • 18.5 印张 • 456 千字

0001－5000 册

定价：28.00 元

前　言

《网管员世界》月刊是由中国电子信息产业发展研究院（CCID）创办的网络技术专业媒体，其读者以网络管理技术人员（网管员）为主，辐射网络管理主管、网络爱好者、准网管和所有关注网络事业发展的人士。《网管员世界》内容以技术应用为主，注重实用性和知识性，以帮助网管员解决日常工作中碰到的实际问题，为网管员排忧解难。由于其内容非常契合广大网管员的实际工作需求，创刊不久，就获得了网络界各方面人士的认可，邮局订阅量直线攀升。众多的网管员纷纷来电来函要求购买已出版的全套《网管员世界》杂志。

为了方便网管员朋友从几十本刊物中寻找所需资料，便于收藏保管，经《网管员世界》编辑部全体编辑精挑细选，集网络管理精华的《<网管员世界>精华本》面世了。本书收集了《网管员世界》自创刊以来受到网管员朋友欢迎的众多作品，主要是与网管员的日常工作密切相关的 100 多篇文章，按照新的体系重新排版印刷，内容涵盖了网络管理的方方面面。全书共分五篇：网络设备、Windows 系统维护及应用、Linux 系统维护与应用、数据库、网络安全；同时，考虑到一些读者的需求，增加了全新的附录——ADSL 全攻略。本书可作为网管员的工作手册，在工作中遇到问题时随时查找；或作为一般网管员充实提高的进阶工具，在工作之余进行研习；本书也可作为广大网络爱好者和其他网络从业人员探索网络技术的工具书或参考资料。

参加本书编辑的人员有：邢藏菊（第 1 篇）、孙高峰（第 2 篇）、余前帆（第 3 篇）、边歆（第 4 篇）、杨文飞（第 5 篇、附录）。《网管员世界》月刊执行总编胡万进在百忙之中对本书进行了审阅。由于时间紧张，加之编者水平所限，书中错误之处难免，欢迎读者批评指正，以利于我们今后改进。

《网管员世界》杂志社

目　录

第1篇 网络设备

1.1 设备互联与配置

安装、维护 Cisco 路由器的一般方法

乐时进 徐 亮

Cisco 路由器作为网络通信的核心设备，得到了广泛的应用。下面就介绍一下笔者在实践中总结出的经验。

1．控制口接口的做法及连接

将 Cisco2500/1000 系列路由器附件中的控制电缆 RJ45 的一端连接到 Cisco 的 CONSOLE 口上，Cisco7000/4000 系列路由器则将 MODEM 电缆的 DB25 的一端接到 Cisco 的 CONSOLE 口上，DB9 的一端连接到 PC 的 COM1/2 上。在 PC 上设置仿真终端程序：比如用 Windows 中的 TERMINAL 程序，使用 COM1/2，9600BPS，8 DATA BIT，2STOP BIT，其余使用默认值。做好控制口连接后，打开路由器的电源开关。

2．初始化安装

路由器必须使用带有有效接地的电源。一般要求使用的电源的零地间的电压小于 4 伏，零火/地火的电压就为 220 伏。地线保护基本上要求上网的设备需有保护地线，这些设备包括主机、工作站、集线器、交换机、路由器及连接路由器的 MODEM 等。配置路由器的终端或 PC 机也必须使用带有有效接地的电源。Cisco 的同步串行接口是多用的，通过不同的电缆可引出不同的接口，如 RS232、V.35 等，并且 Cisco 的同步串行接口电缆的电缆是特别预制的。第一次安装时系统会自动进入 DIALOG SETUP 状态，依次回答路由器名称、加密超级登录密码、超级登录密码、远程登录密码、动态路由协议、各个接口的配置等。之后回答 YES 保存该配置。然后等 2 分钟，按回车键数下。出现路由器名称，打入 ENABLE 命令，回答超级登录密码，出现路由器名称。

3．对同步拨号、专线、DDN 连接进行配置

以下是在路由器上对这些项目进行配置的命令行：

IPX routing IPX routing
INTERFACE SERIAL 0 INTERFACE SERIAL 0
IP ADDRESS 1.1.1.1 255.0.0.0 IP ADDRESS 1.1.1.2
255.0.0.0
IPX NETWORK 111 IPX
NETWORK 111
INTERFACE ETHERNET 0 INTERFACE ETHERNET 0

IP ADDRESS 12.1.1.1 255.0.0.0 IPADDRESS 16.1.1.1
255.0.0.0
IPX NETWORK 123456 IPX
NETWORK 987654

ROUTER IGRP 1 ROUTER
IGRP 1
NETWORK 1.0.0.0 NETWORK 1.0.0.0
NETWORK 12.0.0.0 NETWORK
16.0.0.0

VPN 在路由器上的实现

庄一嵘

虚拟专用网络（Virtual Private Network，简称 VPN）能够利用 Internet 或其他公共互联网络的基础设施为用户创建隧道，并提供与专用网络一样的安全和功能保障。

一般情况下，VPN 可以用于允许远程通信方，包括销售人员或企业分支机构使用 Internet 等公共互联网络的路由基础设施以安全的方式与位于企业局域网端的企业服务器建立连接。同样的，对于网管人员来说，他们也因此多一种选择，而且是一种安全的选择，因为他们可以通过公网走 VPN 隧道对企业内部网络资源进行访问和维护。考虑到设备投入最小化的要求，以及对网络拓扑状态和性能影响最小的原则，网管人员可以利用现有的网络资源在不改变网络拓扑的情况下，在边界路由器上部署 VPN，另外由于维护人员对内部资源的访问流量一般不大的现实，因此在边界路由器上开放的 VPN 功能对于网络性能影响不大。下面以 Cisco 2600 路由器为例介绍配置法。

1．拓扑结构

拓扑结构比较简单，企业一般是由一台 Cisco 中端产品作为边界路由器（见图 1.1-1）。

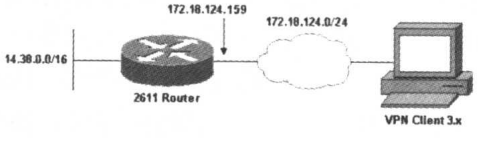


图　1.1-1

这里以 Cisco 2611 路由器作为边界路由设备。

在 Cisco 技术支持网站上有其详细的配置，这里将就主要的配置做详细的说明。具体配置可以参考：

http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_configuration_example09186a0080094847.shtml。

根据 VPN 建立过程，可以划分为以下三个阶段。

第一阶段，IKE 协商。IKE 协商主要涉及密钥交换方式，采用加密算法。一般来讲，会有以下参数需要设置：加密算法、散列函数（Hash）和认证方式。

在具体配置 Cisco 路由器的时候，应首先建立 ISAKMP 策略集，然后依次配置其加密算

法、散列函数和认证方式。下面是从 Cisco 技术支持网站的 Running-config 摘下来的，请参考。

```
crypto isakmp policy 3
encr des
authentication pre-share
group 2
```

说明："encr des" 表示加密采用 des 算法，注意在国内只有 des 算法可以用，因为美国对加密有出口限制。"authentication pre-share" 表示初始协商时使用预先设置的共享密钥。密钥的具体配置在后面配置 VPN 用户组参数时配置。

第二阶段，用户组配置。用户组的配置主要是对发出请求接入的用户进行初始化协商、身份确认、分配 IP 资源，以及告知用户其内部网络支撑系统资源配属情况。一般涉及下列参数：初始化协商所需的密钥、用户认证方式、用户可以使用的 IP 地址资源、用户接入内部网络后其 DNS、WINS、域名后缀等基本信息参数。

```
crypto isakmp client configuration group 3000client
key cisco123
dns 14.1.1.10
wins 14.1.1.20
domain cisco.com
pool ippool
```

由于我们采用的是共享密钥方式，因此，在这里需要设置 key 的具体值。另外，pool 设置可以参照下面实例。

```
ip local pool ippool 14.1.1.100 14.1.1.200
```

第三阶段，用户信道参数。用户信道参数的设置是对用户建立 VPN 通道可以采用的算法集合进行界定，以方便通信双方协商其具体通信过程中所采用的加密算法，并建立映射关系。一般需要设置 transform-set 和 map 集。

```
crypto dynamic-map dynmap 10
set transform-set myset
!
crypto map clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list groupauthor
crypto map clientmap client configuration address respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
```

需要说明的是，VPN 组网方式有两大类：Peer-to-Peer 和 Point-to-Peer 的方式。这里选择的是后者，其特点是用户 IP 是动态的，因此，这里的映射集合应该为动态的。另外，这里具体配置了用户认证的方式，为使用本地用户数据库认证。具体配置为：

```
aaa new-model
!
aaa authentication login userauthen local
```

```
aaa authorization network groupauthor local
!
username cisco password 0 cisco
```

其中，用户名为 cisco，口令为 cisco。

transform-set 的配置可以参考如下配置：

```
crypto ipsec transform-set myset esp-des esp-sha-hmac
```

2. 需要注意的问题

古人云："尽信书不如无书"。如果完全按照技术资料，即 Cisco 网站由 TAC 确认的配置文件进行配置是不能配通的。原因很简单，因为"show running-config"命令没有将全部的配置显示出来，有些配置可能因为是默认的缘故，或者 Cisco 出于某些考虑，将部分配置信息过滤掉了。

主要的缺漏有：散列函数，hash md5，表明使用 md5 算法对信息进行摘要计算。传输模式，crypto ipsec transform-set myset mode transport 使用透明模式，另外一种模式是 tunnel 模式。

另外，还有以下问题需要注意。

（1）路由问题。需要将接入用户的 IP 路由信息进行配置，否则将不能访问内部服务器，而只能 ping 通网关。可以采用加静态路由方式，给 VPN 地址池用户的 IP（14.1.1.100～14.1.1.200）指明 VPN 网关的接口为其默认路由关口。

```
ip route   14.1.1.0 255.255.255.0 FastEthernet0/0
```

其中 FastEthernet0/0 为 172 网段所在的外口。

（2）边界安全影响。通常情况下，一般网络边缘会配置一定的网络访问控制策略。如果配置了拒绝 UDP 协议或者只允许部分 UDP 端口访问的策略的话，那么会影响 VPN 通道的建立。因为 IKE 协商时会使用 UDP 500 端口进行协商。因此，还需要开放必要的端口资源，具体配置请参阅有关资料。

笔者学校最近对校园主干网进行了改造，路由器使用的是 Cisco 2621，中心交换机使

1. 基于端口的 VLAN 划分

基于端口的 VLAN 在逻辑上是由一个或多个交换机上的端口所组成，每个端口被指定为一个 VLAN 接口。3Com 4900 预先定义了一个基于端口的 VLAN，它最初包括所有端口。

（1）VLAN 标识（VID）的概念。对于用户创建的 VLAN，系统利用其 VLAN 标识号（VID）对其进行跟踪。在 VLAN 的具有标记功能的端口，由系统发送的数据帧通过 IEEE 802.1q 标准进行标记。系统接收的标记过的数据帧被分配给在标记中包含相应 VID 的 VLAN。当端口被标记时，该端口可以属于几个 VLAN。通常情况下，默认 VLAN 的 VID 为 1，用户创建 VLAN 的 VID 编号范围为 2～2048。

（2）基于端口的 VLAN 配置。用户在配置基于端品的 VLAN 时，一定要弄明白 VLAN 接口（Interface）和端口标记的概念。

1）VLAN 接口是虚拟网的逻辑路由端口，每个虚拟网都必须设置一个 VLAN 接口，对于一台 3Com 4900 交换机，VLAN 接口可以看作是交换模块上的虚拟路由接口，甚至可以把 VLAN 接口看作一台路由器上的 IP 接口。网络管理人员可以根据需要控制 VLAN 接口的配置。因此可以这样说，定义 VLAN 接口实际上是定义各 VLAN 子网之间通信的路由接口。

2）VLAN 的接口 IP 地址只能在 3Com 4900SX 中定义，每一个 VLAN 应定义一个接口 IP 地址，并且要注意分配的接口 IP 地址必须属于相对应的 VLAN 的网段上。

3）确定希望所指定的 VLAN 接口中的哪些端口可以被其他 VLAN 接口共享。共享的端口会产生重叠的 VLAN，不共享端口会产生不重叠的 VLAN。

4）重叠的 VLAN 端口需要标记，即如果端口和另一个 VLAN 重叠时，我们需要通过标记的手段加以区分。

2. 网络模型

下面为了说明方便，笔者以一个简单的网络模型为例，详细阐述如何设置 3Com 交换机（见图 1.1-2）。

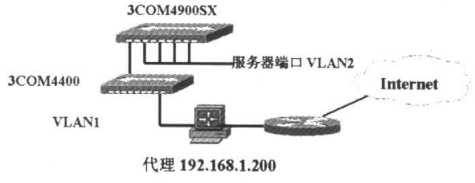


图 1.1-2

（1）3Com 4900SX 上有 12 个 1000M 光纤口，在这里我们只使用其中的 5 个端口，其中 1 号端口我们通过 1000M 光纤和 3Com 4400 上的一个 1000M 光纤模块 25 号端口相连，2～5 号端口通过光纤网卡连接到服务器上。

（2）我们把 3Com 4900SX 上的 2～5 号端口设置成 VLAN2 子网，而把 1 号端口和 4400 交换机上的 25 个端口（24 个 100M 口以及一个扩展的一个 1000M 端口）设置成 VLAN1 子网。假设 VLAN1 子网为 192.168.1.0/24，VLAN2 子网为 192.168.2.0/24。

（3）网络内计算机通过代理（192.168.2.100）访问 Internet。

3. 配置交换机

（1）配置方式的建立。3Com 4400 交换机的配置方式与 3Com 4900 类似，这里以 3Com

4900 为例。

方法 1，可以使用该交换机前面板上提供的 Terminal 控制口进行配置交换机，将 Console 线一端连到交换机 Terminal 控制口上，另一端连到一台计算机的串口上，在 Windows 9X 或 Windows 2000/XP 上启动超级终端程序。注意串口的属性设置为：每秒位数 9600，数据位为 8，奇偶检验为无，停止位为 1，数据流控制为无。

方法 2，因为 3Com 4900 在出厂前默认的 IP 地址是 192.254.100.100/24，所以您只需先设置一台客户机使其处于同一个网段，然后在客户机上使用 Telnet 192.254.100.100，您就可以进入到 3Com 4900 交换机的配置登录界面。

方法 3，在 IE 浏览器的地址栏中输入 192.254.100.100，您也可以进入到 3Com 4900 交换机的配置登录界面。

（2）为交换机分配 IP 地址。进入配置主菜单后，应首先修改密码，然后设置交换机 IP，一般在整体网络规划时将交换机划分成一个独立的子网，在这里我们设成 3Com 4900 的 IP 为 192.168.20.6。进入 protocol/ip/basicConfig，输入分配给交换机的 IP 地址为 192.168.20.6，掩码为 255.255.255.0，网关为 192.168.1.200。同样我们进入到 3Com 4400 交换机上将其 IP 地址设置为 192.168.20.9/24。

（3）定义 VLAN-1 和 VLAN-2。由主菜单进入 bridge/vlan/，可以使用“summary”命令查看所定义的 VLAN，3Com 4900 和 3Com 4400 系统中已经建立了一个名称为 default VLAN 的 VLAN。它包括所有的端口，我们可以使用“create”命令定义新的 VLAN。先定义名字为 VLAN-1 的一个 VLAN，再使用同样的方法增加 VLAN-2，完成后，使用“summary”命令查看结果（见表 1.1-1）。

表 1.1-1

VLANID	Name
1	Default VLAN
2	VLAN-1
3	VLAN-2

完成上述任务后，还需在 3Com 4400 上建立一个名为 VLAN-1 的 VLAN。

（4）给 VLAN 分配端口。在 3Com 交换机上建立 VLAN 后，下一步就应该给 VLAN 绑定端口，在默认的情况下，3Com 4900 和 4400 交换机上的所有端口都属于 Default VLAN，因此应按网络规划要求给新建的两个 VLAN 绑定端口。

1）将 3Com 4900SX 上 1 端口分配给 VLAN1，将 2～5 端口分配给 VLAN2（服务器端口），由主菜单进入 bridge/vlan/modify/addport：

```
Select VLAN ID (1-3)[1]:2
Select bridge port(1-12,AL1-AL4,all)[all]:1
Enter tag type(untagged,tagged): untagged
```

当系统中存在被不同的 VLAN 共享的端口时，用户必须采用标记，以便区分共享的端口。在本例中因为端口没有被复用，所以不用标记。重复上面的操作将 2～5 端口分配给 VLAN2。

2）将 3Com 4400 上 1～25 端口分配给 VLAN1。

（5）定义 VLAN 的接口的 IP 地址。如果要实现 2 个 VLAN 之间的通信，必须为每一个 VLAN 分配接口 IP 地址，从主菜单进入 protocol/ip/interface/add，定义 VLAN 的接口 IP 地址，并且要注意分配的接口 IP 地址必须属于相对应的 VLAN 的网段，否则定义失败。例

如，下面是为 VLAN-1 定义接口 IP 地址。

```
Enter IP address:192.168.1.1
Enter subnet mask:255.255.255.0
Enter associated VLAN ID(1-3)[1]:2
Enter type of IP address(primary,secondary)[ primary]: primary
```

这样在 VLAN2 上的所有机器均通过 3Com 4900 上的逻辑路由接口 192.168.1.1 来实现与其他 VLAN 的通信。有时一个 VLAN 是由几个网段组成的，就应配置几个 Interface，其中一个是 primary 接口，其余的都是 secondary 接口。在本例中没有考虑由多网段组成一个 VLAN 的情况。因此就不需设置类型为“secondary”的路由接口。

采用同样的方法，定义 VLAN-2 的接口 IP 地址为“192.168.2.1”。使用 summary 命令查看结果（见表 1.1-2）。只要有计算机联到 VLAN 中的端口上，其 VLAN 的状态即为 UP。

表 1.1-2

IndeX	Type	IP address	Subnet	state	VLAN ID
1	primary	192.168.20.6	255.255.255.0	Up	1
2	primary	192.168.1.1	255.255.255.0	Up	3
3	primary	192.168.2.1	255.255.255.0	Up	2

（6）为交换机增加默认网关。连入交换机的计算机如果想访问 Internet，就需要给交换机分配一个默认路由。从主菜单进入 protocol/ip/router/default，定义默认路由，此地址是局域网内路由器的 IP 地址或代理服务器的 IP 地址。

```
Enter gateway IP address: 192.168.1.200
```

这样，网络内的计算机可以访问 Internet 了。

4．设置 VLAN 中的计算机

位于 VLAN 中的计算机，除了设置本网段的 IP 地址外，如果想访问其他 VLAN 或其他网段的计算机和网络设备，需要在计算机中设置默认网关，其网关为本 VLAN 的接口地址。例如 VLAN-1 中的计算机，其网关应设置为 192.168.1.1，掩码为 255.255.255.0，VLAN-2 中的网关应设置为 192.168.2.1，掩码为 255.255.255.0。

交换机镜像端口的工作原理及配置方法

赵新启

对于高级网管员来说，在进行网络故障排查、网络数据流量分析的过程中，有时需要对网络节点或骨干交换机的某些端口进行数据流量监控分析，而在交换机中设置镜像端口，对某些可疑端口进行监控，同时又不影响被监控端口的数据交换，已成为常用的解决方案之一。本文以 Cisco Catalyst 4006 交换机为例介绍“交换端口分析器”的工作原理及配置方法。

1．SPAN 工作原理

SPAN（Switched Port Analyzer）的作用主要是为了给某种网络分析器提供网络数据流。

它既可以实现一个 VLAN 中若干个源端口向一个监控端口镜像数据，也可以从若干个 VLAN 向一个监控端口镜像数据。源端口的 5 号端口上流转的所有数据流均被镜像至 10 号监控端口，而数据分析设备通过监控端口接收了所有来自 5 号端口的数据流（见图 1.1-3）。

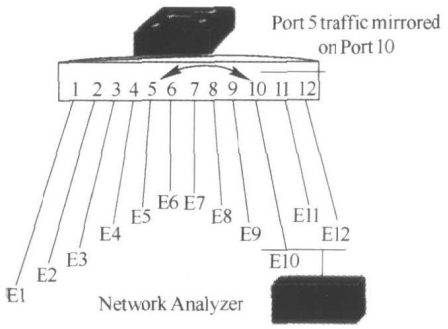


图 1.1-3

值得注意的是，源端口和镜像端口必须位于同一台交换机上（但也有例外，如 Catalyst 6000 系列交换机）；而且 SPAN 并不会影响源端口的数据交换，它只是将源端口发送或接收的数据包副本发送到监控端口。

在 SPAN 任务过程中，用户可以通过参数控制，来指明需要监控的数据流种类；还可以将一个或多个端口、一个或多个 VLAN 作为源端口，并将从这些端口中发送或接收的单向或双向数据流传送至监控端口。

在 Catalyst 4006 交换机中，最多可以配置 6 个单向的 SPAN 任务：2 个输入数据流监控、4 个输出数据流监控。一个双向 SPAN 任务实际上包含一个单向输入和一个单向输出。而且不仅仅二层交换端口可作为源端口，Catalyst 4006 上的三层路由端口也可设置为源端口。

SPAN 任务不会影响交换机的正常工作。当一个 SPAN 任务被建立后，根据交换机所处的不同的状态或操作，任务会处于激活或非激活状态，同时系统会将其记入日志。通过“show monitor session”命令可显示 SPAN 的当前状态。

如果遇到系统重新启动的情况，在目的端口初始化结束之前，SPAN 任务将处于非激活状态。目的端口（监控端口）可以是交换机上的任意一个交换或路由端口。当一个目的端口处于激活状态时，任何发送到该端口且与 SPAN 任务无关的数据包将会被丢弃。

一个目的端口只能处于一个 SPAN 任务中。当一个端口被配制成目的端口后就不能再成为源端口，同时冗余链路端口也不能成为 SPAN 的目的端口。特别需要指出的是，如果一个 Trunk 端口被配置成为 SPAN 的目的端口，则其 Trunk 功能也将自动停止。

源端口又可以称作被监控端口。在一个 SPAN 任务中，可以有一个或多个源端口，而且可以根据用户需要设置为输入方向、输出方向或双向，但无论哪种情况，在一个 SPAN 任务中，所有源端口的被监控方向都必须是一致的。

在 Catalyst 4006 交换机上的 VLAN 也可以整体设置为源端口，这意味着被指定 VLAN 中的所有端口均为当前 SPAN 任务中的源端口。

Trunk 端口可以单独设为源端口，也可以与非 Trunk 端口一起被设置为源端口，但要注意的是，在监控端口不会识别来自 Trunk 端口针对不同 VLAN 的数据封装格式，换句话说，

在监控端口收到的数据包将无法辨明是来自哪个 VLAN。

SPAN 数据流主要分为三类：

（1）输入数据流（Ingress SPAN）：指被源端口接收进来，其数据副本发送至监控端口的数据流；

（2）输出数据流（Egress SPAN）：指从源端口发送出去，其数据副本发送至监控端口的数据流；

（3）双向数据流（Both SPAN）：即为以上两种的综合。

基于 VLAN 的 SPAN 是以一个或几个 VLAN 作为监控对象，其中的所有端口均为源端口，与基于端口的 SPAN 类似，基于 VLAN 的 SPAN 也分为输入数据流、输出数据流和双向数据流监控三种类型。

在配置基于 VLAN 的 SPAN 任务过程中，应注意几点：

（1）Trunk 端口可以包含在源端口中；

（2）针对双向 SPAN 任务，如果在源 VLAN 中的两个源端口之间有数据交换，则每一个数据包将有两个副本被转发至镜像端口；

（3）对有多个源 VLAN 的 SPAN 任务来说，如果某个源 VLAN 被删除掉，则该 VLAN 也将从源 VLAN 列表中删除；

（4）处于非激活状态的 VLAN 无法参与 SPAN 任务；

（5）对于一个设置为输入数据流监控的源 VLAN 来说，来自其他 VLAN 的路由信息数据包不会被镜像；此外，从设置为输出数据流监控的 VLAN 向其他 VLAN 发送出的路由信息数据包也同样不会被镜像。换句话说，基于 VLAN 的 SPAN 任务只对进出二层交换端口的数据包进行镜像，而不镜像 VLAN 之间的路由信息。

所有网间传输的非路由数据包，包括组播包和 BPDU（桥接协议数据单元）包，都可以使用 SPAN 任务进行镜像。

在一些 SPAN 任务的配置下，会出现同一个 SPAN 源端口数据包的多个副本被发送到 SPAN 监控端口的情况。正像前面提到的那样，在一个双向 SPAN 任务中，假设 a1 和 a2 为源端口，d1 为目的端口，如果 a1 与 a2 之间有数据包传输，则在 a1 传向 a2 的数据包将会被传送到 d1 两次，反之亦然。

2. SPAN 的配置方法

在配置 SPAN 任务时应遵循以下原则：

（1）对数据进行监控分析的设备应搭接在监控端口上；

（2）在一个基于 VLAN 的 SPAN 任务中不能同时存在源 VLAN 和过滤 VLAN；

（3）冗余链路端口只能作为 SPAN 任务的源端口；

（4）SPAN 任务中所有的源端口的被监控方向必须一致；

（5）在设置端口为源端口时，如果没有指定数据流的监控方向，默认为双向；

（6）当 SPAN 任务含有多个源端口时，这些端口可以来自不同的 VLAN；

（7）取消某一个 SPAN 任务的命令是：no monitor session 任务号；

（8）取消所有 SPAN 任务的命令是：no monitor；

（9）SPAN 任务的目的端口不能参与到生成树的距离计算中，但由于源端口的 BPDU 包可以被镜像，所以 SPAN 目的端口可以监控到来自源端口的 BPDU 数据包。