# 第 3 章　交换机技术

## 3.1　交换机概述

### 3.1.1　交换机的定义

交换(Switching)是按照通信两端传输信息的需要,用人工或设备自动完成的方法,把要传输的信息送到符合要求的相应路由上的技术的统称,是为了传送信号,连接功能单元,传输通道或电信电路的过程。表示任何移动数据的过程。交换机是按照通信两端传输信息的需要,用人工或设备自动完成的方法,把要传输的信息送到符合要求的相应路由上的技术的统称。广义的交换机就是一种在通信系统中完成信息交换功能的设备,它工作 OSI 参考模型的第二层——在数据链路层,主要功能包括物理编址、网络拓扑结构、错误校验、帧序列以及流控。交换机有多个端口,每个端口都具有桥接功能,可以连接一个局域网或一台高性能服务器或工作站。实际上,交换机有时被称为多端口网桥。

在计算机网络系统中,交换概念的提出改进了共享工作模式。而 Hub 集线器就是一种 OSI 参考模型的第一层——物理层的共享设备,Hub 本身不能识别 MAC 地址和 IP 地址,当同一局域网内的 A 主机给 B 主机传输数据时,数据包在以 Hub 为架构的网络上是以广播方式传输的,由每一台终端通过验证数据报头的 MAC 地址来确定是否接收。也就是说,在这种工作方式下,同一时刻网络上只能传输一组数据帧的通信,如果发生碰撞还得重试。这种方式就是共享网络带宽。通俗地说,普通交换机是不带管理功能的,一根进线,其他接口接到电脑上就可以了。

交换机拥有一条很高带宽的背部总线和内部交换矩阵。交换机的所有端口都挂接在这条背部总线上,控制电路收到数据包以后,处理端口会查找内存中的地址对照表以确定目的 MAC 地址(IEEE 局域网所采用的二层地址,例如网卡的硬件地址)的设备挂接在哪个端口上,通过内部交换矩阵迅速将数据包传送到目的端口,目的 MAC 地址若不存在才广播到所有的端口,接收端口回应后交换机会“学习”新的地址,并把它添加到内部 MAC 地址表中。交换机也可以把网络“分段”,通过对照 MAC 地址表,交换机只允许必要的网络流量通过交换机。通过交换机的过滤和转发,可以有效地隔离广播风暴,减少误包和错包的出现,避免共享冲突。交换机在同一时刻可进行多个端口对之间的数据传输。每一端口都可视为独立的网段,连接在其上的网络设备独自享有全部的带宽,无须同其他设备竞争使用。即:当节点 A 向节点 D 发送数据时,节点 B 可同时向节点 C 发送数据,而且

这两个传输都享有网络的全部带宽，都有着自己的虚拟连接，假使这里使用的是 100Mb/s 的以太网交换机，那么该交换机这时的总流通量就等于 2×100Mb/s＝200Mb/s，而使用 10Mb/s 的共享式 Hub 时，一个 Hub 的总流通量也不会超出 10Mb/s。因此，交换机是一种基于 MAC 地址识别，能完成封装转发数据包功能的网络设备。交换机可以“学习”MAC 地址，并把其存放在内部地址表中，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源地址到达目的地址。

### 3.1.2　交换机的常见分类

(1) 从广义上来看，网络交换机分为两种：广域网交换机和局域网交换机。广域网交换机主要应用于电信领域，提供通信用的基础平台。而局域网交换机则应用于局域网络，用于连接终端设备，如 PC 及网络打印机等。

(2) 根据传输介质和传输速度可分为以太网交换机、快速以太网交换机、千兆以太网交换机、万兆以太网交换机、十万兆以太网交换机、FDDI 交换机、ATM 交换机和令牌环交换机等。

目前以太网类交换机应用最为广泛，本文也将以以太网类交换机为主要讲授内容。

(3) 根据规模应用又可分为企业级交换机、部门级交换机、工作组交换机、桌机型交换机等。

(4) 根据交换机端口结构划分固定端口交换机和模块化交换机。固定端口交换机只能提供有限数量的端口和固定类型的接口(如 100Base-T、1000Base-T、GBIC、SFP 插槽、万兆插槽)。一般的端口标准是 8 端口、16 端口、24 端口、48 端口等，如图 3-1 所示。模块化交换机拥有更大的灵活性和可扩充性，用户可任意选择不同数量、不同速率和不同接口类型的模块，以适应千变万化的网络需求，如图 3-2 所示。

图 3-1　固定端口交换机

(5) 根据层次分类，交换机可分为二层交换机、三层交换机、四层交换机等。

二层交换设备工作在 OSI 模型的第二层，即数据链路层，它对数据包的转发是建立在 MAC(Media Access Control)地址的基础之上的。二层交换设备不同的接口发送和接收数据独立，各接口属于不同的冲突域，因此有效地隔离了网络中的物理层冲突域，使得通过它互连的主机(或网络)之间不必再担心流量大小对于数据发送冲突的影响。

二层交换设备通过解析和学习以太网帧的源 MAC 来维护 MAC 地址与接口的对应关系(保存 MAC 与接口对应关系的表称为 MAC 表)，通过其目的 MAC 来查找 MAC 表决定向哪个接口转发，基本流程如下：

二层交换设备收到以太网帧，将其源 MAC 与接收接口的对应关系写入 MAC 表，作为以后的二层转发依据。如果 MAC 表中已有相同表项，那么就刷新该表项的老化时间。

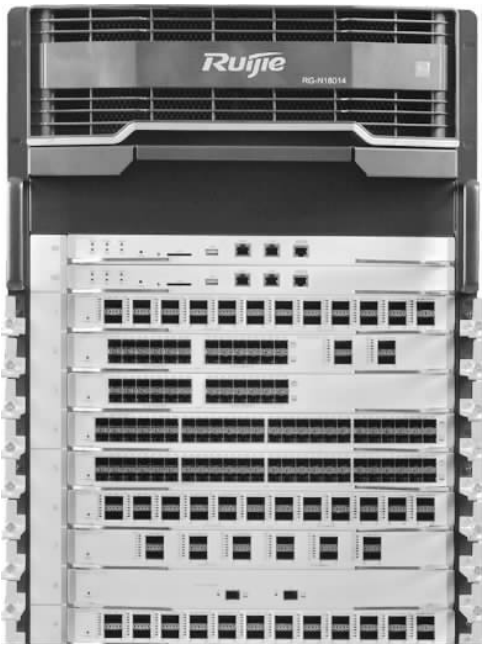


图 3-2 模块化端口交换机

MAC 表表项采取一定的老化更新机制，老化时间内未得到刷新的表项将被删除掉。根据以太网帧的目的 MAC 去查找 MAC 表，如果没有找到匹配表项，那么向所有接口转发（报文的入接口除外）；如果目的 MAC 是广播地址，那么向所有接口转发（报文的入接口除外）；如果能够找到匹配表项，则向表项所示的对应接口转发。

从上述流程可以看出，二层交换通过维护 MAC 表以及根据目的 MAC 查表转发，有效地利用了网络带宽，改善了网络性能。

二层交换设备虽然能够隔离冲突域，但是它并不能有效地划分广播域。因为从前面介绍的二层交换设备转发流程可以看出，广播报文以及目的 MAC 查找失败的报文会向除报文的入接口之外的其他所有接口转发，当网络中的主机数量增多时，这种情况会消耗大量的网络带宽，并且在安全性方面也带来一系列问题。当然，通过路由器来隔离广播域是一个办法，但是由于路由器的高成本以及转发性能低的特点使得这一方法应用有限。基于这些情况，二层交换中出现了 VLAN 技术。

三层交换机可以工作在网络层，它比二层交换机更加高档，功能更加强。它具有路由功能，它将 IP 地址信息提供给网络路径选择，并实现不同网段间数据的线速交换。目前的三层交换机一般是通过 VLAN 来划分二层网络并实现二层交换的，同时能够实现不同 VLAN 间的三层 IP 互访。

路由器与三层交换机的简单区别：路由器的三层转发主要依靠 CPU 进行，而三层交换机的三层转发依靠硬件完成，能实现高速三层转发，这就决定了两者在转发性能上的巨大差别。三层交换机并不能完全替代路由器，路由器所具备的丰富的接口类型、良好的流量服务等级控制、强大的路由能力等仍然是三层交换机的薄弱环节。

四层交换机支持 TCP/UDP 第四层以下的所有协议，可识别至少 80 个字节的数据包包头长度，可根据 TCP/UDP 端口号来区分数据包的应用类型，从而实现应用层的访问控制和服务质量保证。所以，与其说第四层交换机是硬件网络设备，还不如说它是软件网络管理系统。也就是说，第四层交换机是一类以软件技术为主，以硬件技术为辅的网络管理交换设备。

(6) 根据是否支持网管功能划分网管型交换机和非网管理型交换机。网管型交换机，也称智能交换机，它拥有独立的操作系统，可以进行配置与管理。不能进行配置与管理的交换机称为不可网管交换机。

(7) 根据承载功能和放置位置可分为接入层交换机、汇聚层交换机和核心层交换机。部署在接入层的交换机就称为接入层交换机。通常为固定端口交换机，用于实现终端计算机的网络接入。接入层交换机可以选择拥有 1～2 个 1000Base-T 端口、GBIC、SFP 或万兆插槽的交换机，用于实现与汇聚层交换机的连接。部署在汇聚层的交换机称为汇聚层交换机，也称骨干交换机、部门交换机，是面向楼宇或部门接入的交换机。汇聚层交换机首先汇聚接入层交换机发送的数据，再将其传输给核心层，最终发送到目的地。汇聚层交换机可以是固定端口交换机，也可以是模块化交换机，一般配有光纤接口。部署在核心层的交换机称为核心层交换机，也称中心交换机。核心层交换机属于高端交换机，一般全部采用模块化结构的可网管交换机，作为网络骨干构建高速局域网。

### 3.1.3　交换机的主要性能指标

#### 1. 模块插槽及业务板类型

模块插槽主要指交换机支持的业务槽位数、交换网槽位数，业务槽位主要用于交换机安装如接入、交换、路由等业务板卡需要，交换网槽位主要用于安装主控处理单元、交换单元或管理引擎模块等，如 3 槽位、7 槽位、10 槽位、14 槽位等。交换机业务板类型越丰富越有利于根据实际选择组网，例如：12 端口千兆/万兆以太网光接口板(SFP/SFP+)、48 端口百兆/千兆以太网光接口板(SFP)、4 端口 100Gb/s 以太网光接口板(CFP)、防火墙业务处理板等。

#### 2. 交换容量

交换容量也称为背板带宽或交换带宽。交换容量是交换机接口处理器(或接口卡)和数据总线之间所能吞吐的最大数据量。背板带宽标志了交换机总的数据交换能力，单位为 Gb/s。一台交换机的交换容量越高，所能处理数据的能力就越强。所有端口容量、端口数量之和的两倍应该小于交换容量，从而实现全双工无阻塞交换。如锐捷的 RG-N18010 和华为的 CE12808S 交换机，交换容量达 32Tb/s，并可升级至 80Tb/s。

#### 3. 包转发率

包转发率也称为端口吞吐量，是指通信设备某端口上的数据包转发能力，单位通常使用 pps(packet per second)来衡量。通常低端设备的包转发率只有几 kpps 到几十 kpps，而高端设备则能达到几十、几百、几千甚至上万 Mpps。如锐捷的 RG-N18010 和华为的

CE12808S 交换机，包转发率达 14400Mpps。

**4. 以太业务性能**

以太业务性能主要包括支持以太网接口属性、VLAN 功能、MAC 地址功能，支持 STP、RSTP、MSTP、GVRP 协议等性能指标。

**5. IP 性能**

IP 性能主要包括支持 ARP、DHCP 等功能，支持 RIP、OSPF、ISIS、BGP、IPv4 动态路由协议，支持策略路由以及支持 RIPng、OSPFv3、ISISv6、BGP4＋等 IPv6 动态路由协议，支持 IPv6 策略路由，支持手工隧道、自动隧道、ISATAP 隧道、支持 GRE 隧道，支持 IPv6 ND、支持 PMTU 发现、支持 IPv6 的 TCP、Ping、Tracert、Socket、UDP、RawIP 等性能指标。

**6. 组播性能**

组播性能主要包括支持 IGMP v1，v2，v3、支持 IGMP Snooping、支持 IGMP Proxy、支持 PIM-DM、PIM-SM、PIM-SSM 等组播路由协议、支持组播成员接口快速离开、支持组播流量抑制等性能指标。

**7. 多协议标签交换性能**

多协议标签交换（MPLS）性能主要包括支持 MPLS 基本功能及支持 MPLS VPN/VPLS /VPLS over GRE 等。

**8. 可靠性**

可靠性主要包括独立的交换网板与独立的主控板设计，实现转发与控制平面完全分离、主控板支持 1＋1 冗余备份、交换网板支持 $N+1$ 冗余备份、电源、风扇支持 $N+M$ 冗余备份、各组件支持热插拔、支持热补丁功能，可在线进行补丁升级、支持 ISSU、支持 GR for OSPF/IS-IS/BGP、支持 BFD for VRRP/OSPF/BGP4/ISIS/ISISv6/MPLS/静态路由等，故障倒换完成时间、拓扑收敛速度等。

**9. QoS 性能**

QoS 性能主要包括支持基于 Layer2、Layer3、Layer4 优先级等的组合流分类、支持 ACL、CAR、Remark 等动作、支持 PQ、WFQ、PQ＋WFQ 等队列调度方式、支持 WRED、尾丢弃等拥塞避免机制、支持流量整形等。

### 3.1.4 交换机的接口

接口是网络设备之间交换数据并相互作用的部件，分为物理接口和逻辑接口两类。物理接口是真实存在、有器件支持的接口，需要承载业务，分为负责承载业务传输的业务接口和负责承载管理业务的管理接口，例如 GE 业务接口和 ETH 管理接口。逻辑接口是指能够实现数据交换功能但物理上不存在、需要通过配置建立的接口，需要承担业务传输，例如 VLANIF 接口、Loopback 接口，常见的逻辑接口如表 3-1 所示。

表 3-1　常见的逻辑接口

| 接口类型 | 描　述 |
| --- | --- |
| Eth-Trunk 接口 | 具有二层特性和三层特性的逻辑接口，把多个以太网接口在逻辑上等同于一个逻辑接口，比以太网接口具有更大的带宽和更高的可靠性 |
| Tunnel 接口 | 具有三层特性的逻辑接口，隧道两端的设备利用 Tunnel 接口发送报文、识别并处理来自隧道的报文 |
| MTunnel 接口 | MTunnel 接口是一种逻辑接口，简称 MTI。MTI 是 MT(Multicast Tunnel)的入/出口，本地 PE(Provider Edge)将私网数据从 MTI 发出，远端 PE 从 MTI 接收私网数据 |
| VLANIF 接口 | 具有三层特性的逻辑接口，通过配置 VLANIF 接口的 IP 地址，实现 VLAN 间互访 |
| 逻辑集群端口 | 逻辑集群端口是专用于集群功能的逻辑端口，将多台支持集群特性的交换机设备组合在一起，从逻辑上组合成一台整体交换设备，从而实现数据中心大数据量转发和网络高可靠性 |
| 子接口 | 子接口就是在一个主接口上配置出来的虚拟接口，主要用于实现与多个远端进行通信 |
| Loopback 接口 | 主要应用其接口状态永远是 Up 和可以配置 32 位子网掩码的特性 |
| NULL 接口 | 因为任何送到该接口的网络数据报文都会被丢弃，主要用于路由过滤等特性 |
| Wlan-ESS 接口 | 该接口是一种虚拟的二层接口，类似于 trunk 类型的二层以太网接口，具有二层属性 |
| 虚拟接口模板 VT(Virtual-Tem plate)接口 | 当需要 PPP 协议承载其他链路层协议时，可通过配置虚拟接口模板来实现 |

(1) 根据接口承载的业务功能不同，交换机的以太网接口可以分为：

① 管理接口，主要为用户提供配置管理支持，也就是用户通过此类接口可以登录到设备，并进行配置和管理操作。管理接口不承担数据业务传输。主要包括 Console 口和 ETH 管理接口。Console 口遵循 EIA/TIA-232 标准，接口类型是 DCE，通过该接口和配置终端的 COM 串口连接，用于搭建现场配置环境。ETH 管理接口遵循 10/100BASE-TX 标准，通过和配置终端或网管站的网口连接，用于搭建现场或远程配置环境，主要为用户提供配置管理支持也就是用户通过此类接口可以登录到设备，并进行配置和管理操作。ETH 管理接口不承担数据业务传输。

② 业务接口，主要承担业务数据的接收和发送。

(2) 根据业务接口支持的速率，交换机的以太网接口可以分为：FE 接口(快速以太网接口)、GE 接口(千兆以太网接口)、XGE 接口(目前是指 10GE 接口或 ACU2 单板上的 20GE 接口)、40GE 接口、100GE 等。常见以太网接口支持情况如表 3-2 所示。

(3) 根据业务接口的电器属性，交换机的以太网接口可以分为：电接口，光接口。

表 3-2 常见以太网接口支持情况

| 接口类型 | 连接介质 | 速率/(Mb/s) | 双工模式 | 自协商模式 | 流量控制 |
|---|---|---|---|---|---|
| FE 电接口 | 网线 | 10 | 全双工/半双工 | 支持 | 支持 |
| | | 100 | 全双工/半双工 | | |
| GE 电接口 | 网线 | 10 | 全双工/半双工 | 支持 | 支持 |
| | | 100 | 全双工/半双工 | | |
| | | 1000 | 全双工 | | |
| FE 光接口 | FE 光模块 | 100 | 全双工 | 不支持 | 支持 |
| GE 光接口 | FE 光模块 | 100 | 全双工 | 不支持 | 支持 |
| | GE 光模块 | 1000 | 全双工 | 支持 | 支持 |
| | GE 光电模块 | 1000 | 全双工/半双工 | 支持 | 支持 |
| XGE(10GE)光接口 | XGE 光模块 | 10000 | 全双工 | 不支持 | 支持 |
| | GE 光模块 | 1000 | 全双工 | 支持 | 支持 |
| | GE 光电模块 | 1000 | 全双工 | 支持 | 支持 |
| 40GE 光接口 | 40GE 光模块 | 40000 | 全双工 | 不支持 | 支持 |
| | 高速电缆 | 40000 | 全双工 | 支持 | 支持 |

(4) 根据业务接口的处理报文的转发方式,交换机的以太网接口可以分为:

二层以太网接口。它是一种物理接口,工作在数据链路层。它只能对接收到的报文进行二层交换转发,也可以加入 VLAN,通过 VLANIF 接口对接收到的报文进行三层路由转发。

三层以太网接口。它是一种物理接口,工作在网络层,可以配置 IP 地址。它可以对接收到的报文进行三层路由转发,即可以收发源 IP 和目的 IP 处于不同网段的报文。

## 3.2 交换机等网络设备的配置基础

管理网络设备分为带外管理、带内管理(in-band)两种方式。带内管理方法有 Telnet/SSH、Web、SNMP 等;带外管理有 CON 和 AUX。其中通过 Console 口管理是最常用方式,首次配置时必须使用这种管理方式。

### 3.2.1 配置方法

管理网络设备可以简单地分为带外管理(Out-Of-Band)、带内管理(In-Band)两种方式。所谓带内管理,是指管理控制信息与用户网络的承载业务信息通过同一个物理信道传送,管理控制信息占用业务带宽,常用的方法有 Telnet/SSH、TFTP、Web、SNMP 等;所谓带外管理,就是网络的管理控制信息与用户网络的承载业务信息在不同的物理信道

传送，设备管理控制信息不占用提供业务带宽，常用方法是 CON 和 AUX。

**1. CON**

网络设备一般有一个用于管理的 Console 口，通过 Console 口管理是最常用的带外管理方式，管理员在首次配置网络设备，或者在无法进行带内管理时必须使用这种管理方式。其方法是通过 Console 专用电缆，连接网络设备的 Console 端口与计算机的串口(COM)，利用终端仿真软件(如 Windows 的超级终端)来管理网络设备。

**2. Telnet/SSH**

远程登录是日常管理网络设备最常用的方法，其方法是使用 Telnet、SSH 等网络工具远程登录到网络设备中，对其进行配置和管理，如图 3-3 所示。其中，Telnet 以明文方式传输数据，SSH 采用密文的方式传输数据，具有更高的安全性。

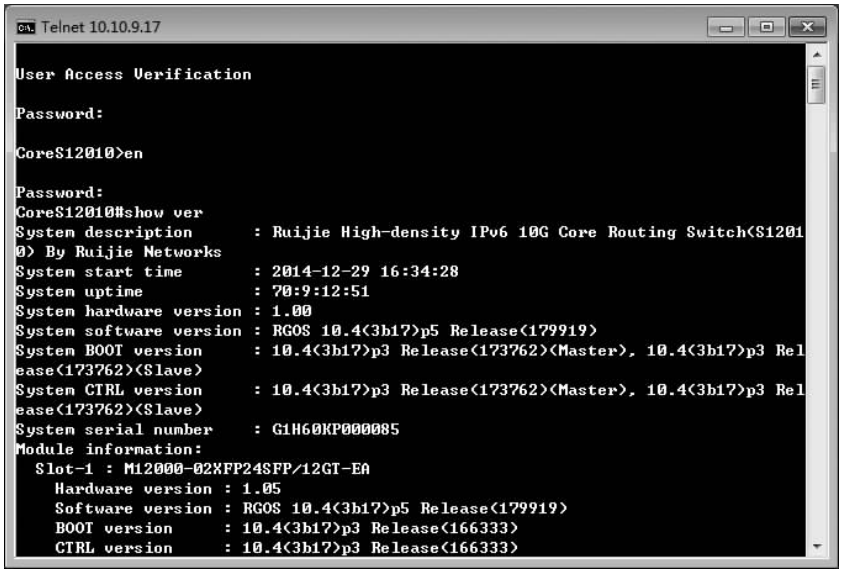


图 3-3　利用 Telnet 远程管理网络设备

使用 CON、Telnet/SSH 管理网络设备时，都是使用类似于 DOS 操作系统下的命令，因此将这种配置界面称为命令行界面(Command Line Interface，CLI)，它与图形化界面(Graphic User Interface，GUI)相对应。CLI 由 Shell 程序提供，由一系列的配置命令组成的，根据这些命令在配置管理网络设备时所起的作用不同，Shell 将这些命令分类，不同类别的命令对应着不同的配置模式。

**3. TFTP**

TFTP 是一种小型化 FTP 服务器，管理员可以从 TFTP 服务器下载网络设备的配置信息，从而达到配置和管理网络设备的目的。TFTP 服务器可以运行在 UNIX 工作站或者 PC 工作站。

**4. SNMP**

SNMP 是简单网络管理协议，通过运行网管软件(如 CiscoWorks)的工作站来管理网

络设备。

**5. AUX**

一些网络设备(如路由器),还可通过辅助(Auxiliary,AUX)端口连接 Modem,让管理员通过电话网与网络设备通信,进行远程配置。

**6. Web**

现在越来越多的网络设备支持通过 Web 方式进行配置和管理,其方法是在网络设备中启用 Web 服务,管理员利用 Web 浏览器连接到网络设备,在图形化界面(GUI)中管理网络设备。与 CLI 方式相比,这种配置方式更容易操作,也不需要记太多的命令,非常适合初级网络管理员,但这种方式配置功能较差,有一些高级配置无法进行。

**7. 通过 Console 口配置网络设备**

在网络设备的各种配置模式中,通过 Console 口配置是最常用的一种配置模式,也是最基本的配置模式。由于 Telnet/SSH、TFTP、SNMP、Web 配置模式都需要预先对网络设备进行相应的配置才能生效,而通过 AUX 口配置模式需要连接 Modem。所以,当第一次对网络设备进行配置时,通过 Console 口配置就是必然的选择。只有先通过 Console 口对网络设备进行配置,才能使用其他的配置方法。另外,由于某些原因造成其他几种配置模式不能对网络设备进行配置和管理时,使用 Console 口对网络设备进行配置就成了唯一的选择。下面详细介绍通过 Console 口配置网络设备的过程。

(1) 连接 Console 电缆。利用随机附带的 Console 电缆,连接网络设备 Console 端口和 PC 的 COM 口,如图 3-4 所示。如果管理 PC(如笔记本电脑)没有 COM 口,可以在电脑配件市场上购买一根 USB 转 COM 口线缆,并安装该电缆的驱动程序,使用 USB 口连接网络设备 Console 端口。

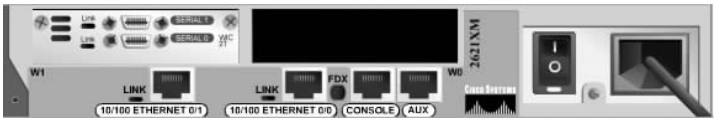


图 3-4 Console 端口

(2) 打开超级终端。打开交换机电源,在已安装“超级终端”的 Windows(以 Windows XP 为例)主机上,依次执行【开始】→【所有程序】→【附件】→【通信】→【超级终端】菜单命令,在打开的【连接描述】对话框,为该超级终端连接指定一个连接名称并选择一个连接图标,单击【确定】按钮,如图 3-5 所示。

(3) 选择 PC 中使用的端口号。在【连接到】对话框中,在【连接时使用】下拉列表中选择使用 PC 的 COM 端口号,单击【确定】按钮,如图 3-6 所示。

(4) 设置超级终端属性。在打开的【COM1 属性】对话框中,单击【还原为默认值】按钮,将【每秒位数】设置为 9600,【数据位】设置为 8,【奇偶校验】设置为“无”,【停止位】设置为 1,【数据流控制】设置为“无”,设置完毕后,单击【确定】按钮,如图 3-7 所示。需要说明一点,这里设置的参数适用于大多数网络设备,如果这个参数不能连接到网络设备,请参阅设备随机说明书,修改相关参数。


图 3-5　【连接描述】对话框


图 3-6　【连接到】对话框


图 3-7　【COM1 属性】对话框

(5) 进入配置命令行模式。当完成超级终端仿真软件的配置后,主机就可以通过 Console 口连接上网络设备,使用 CLI 方式配置和管理网络设备了。如果网络设备正常启动,直接按 Enter 键,进入用户命令模式,如图 3-8 所示。


图 3-8　超级终端

### 3.2.2 主要配置基础

配置基础主要包括使用命令行接口、如何登录设备，以及文件操作、系统启动等功能的配置。

**1. 熟悉命令行**

用户通过命令行对设备下发各种命令来实现对设备的配置与日常维护操作。

**2. 首次登录系统**

当用户需要为第一次上电的设备进行配置时，可以通过 Console 口或 MiniUSB 口登录设备。MiniUSB 口目前只有部分设备支持。

一块主控板提供一个 Console 口（接口类型为 EIA/TIA-232 DCE）和 MiniUSB 口。通过将用户终端的串行口与设备 Console 口直接连接，或者将用户终端的 USB 口与设备 MiniUSB 口直接连接，登录设备，实现对设备的本地配置。

**3. 通过 Console 口登录设备**

PC 端通过设备的 Console 口登录，实现对第一次上电的设备进行基本配置和管理。在配置前需准备好 Console 通信电缆和在 PC 端准备好终端仿真软件。如果 PC 使用系统自带的终端仿真软件（如 Windows 2000/XP 系统的超级终端），则无须另行准备；如果系统不带终端仿真软件，请准备第三方终端仿真软件。

PC 端可能会存在多个连接接口，选择的是连接 Console 线缆的那个接口。一般情况下，选择的接口是 COM1。如果用户 PC 没有可用串口，可以使用 PC 的 USB 口，通过转接线与设备的 Console 口连接。

先使用终端仿真软件通过 Console 口登录设备，然后完成设备的基本配置，详细内容请见 3.2.1 章节中的第 7 种方式即“通过 Console 口配置网络设备”。

**4. 配置用户界面**

当用户通过 Console 口、Telnet 或 SSH 方式登录设备时，系统会分配相应的用户界面，用来管理当前用户与设备之间的会话。

目前设备支持的用户界面有 Console 用户界面和 VTY（虚拟类型终端）用户界面。每个用户界面有对应的用户界面视图。用户界面（User-Interface）视图是系统提供的一种命令行视图，用来配置和管理所有工作在异步交互方式下的物理接口和逻辑接口，从而达到统一管理各种用户界面的目的。

用户界面与用户并没有固定的对应关系。用户登录时，系统会根据用户的登录方式，自动给用户分配一个当前空闲的、编号最小的某类型的用户界面，整个登录过程将受该用户界面视图下配置的约束。例如用户 A 使用 Console 口登录设备时，将受到 Console 用户界面视图下配置的约束，当使用 VTY 1 登录设备时，将受到 VTY 1 用户界面视图下配置的约束。同一用户登录的方式不同，分配的用户界面不同；同一用户登录的时间不同，分配的用户界面可能不同。

(1) Console(CON)。

控制口(Console Port)是一种通信串行口,由设备的主控板提供。一块主控板提供一个 Console 口,接口类型为 EIA/TIA-232 DCE。用户终端的串行口可以与设备 Console 口直接连接,实现对设备的本地访问。

(2) 虚拟类型终端(Virtual Type Terminal,VTY)。

VTY 是一种虚拟线路端口,用户通过终端与设备建立 Telnet 或安全外壳 SSH 连接后,即建立了一条 VTY,即用户可以通过 VTY 方式登录设备。支持多个用户同时通过 VTY 方式访问设备,一般不超过 15 个。

**5. 配置用户登录**

用户可以通过 Console 口、Telnet、STelnet 或者 Web 方式登录设备,实现对设备的本地或远程维护。设备作为服务端时,用户可以通过 Console 口、Telnet、STelnet 或者 Web 方式登录本设备。设备作为客户端时,可以从本设备通过 Telnet 或 STelnet 方式来登录其他设备。

用户对设备的管理方式有命令行方式和 Web 网管方式。

命令行方式:通过 Console 口、Telnet 或 STelnet 方式登录设备后,使用设备提供的命令行对设备进行管理和配置。此种方式需要配置相应登录方式的用户界面。常用的用户登录方式如所表 3-3 所示。

**表 3-3　常用的用户登录方式**

| 登录设备方式 | 优　　点 | 缺　　点 | 应 用 场 景 |
|---|---|---|---|
| Console 口登录 | 使用专门的 Console 通信线缆连接,保证可以对设备有效控制 | 不能远程登录维护设备 | 当对设备进行第一次配置时,可以通过 Console 口登录设备进行配置<br>当用户无法远程登录设备时,可通过 Console 口进行本地登录<br>当设备无法启动时,可通过 Console 口进入 Boot 进行诊断或系统升级 |
| Telnet 登录 | 便于对设备进行远程管理和维护,不需要为每一台设备都连接一个终端,极大地方便了用户的操作 | 传输过程采用 TCP 协议进行明文传输,存在安全隐患 | 终端连接到网络上,使用 Telnet 方式登录设备,进行本地或远程的配置。应用在对安全性要求不高的网络 |
| STelnet 登录 | STelnet 协议实现在不安全网络上提供安全的远程登录,保证了数据的完整性和可靠性,保证了数据的安全传输 | 配置较复杂 | 如果网络对于安全性要求较高,可以通过 STelnet 方式登录设备。STelnet 基于 SSH(Secure Shell)协议,提供安全的信息保障和强大认证功能,保护设备不受 IP 欺骗等攻击 |

Web 网管方式:通过 HTTPS 方式登录设备,设备内置一个 Web 服务器,用户从终端通过 Web 浏览器登录到设备,使用设备提供的图形界面,从而非常直观地管理和维护设备。此种方式必须确保设备上已经加载了 Web 网页文件。Web 网管方式虽然是通过图形界面直观地管理设备,便于用户操作,但提供的是对设备日常维护及管理的基本功

能，如果需要对设备进行较复杂或精细的管理，仍然需要使用命令行方式。

**6. 文件管理**

配置文件、系统软件等文件都保存在设备的存储器中，可通过多种方式实现对存储器中的文件进行管理，同时也可以将当前设备作为客户端，通过多种方式实现对其他设备的文件进行访问。

用户可以通过直接登录系统、FTP、TFTP、SFTP、SCP 和 FTPS 方式进行文件操作，实现对文件的管理，如表 3-4 所示。

**表 3-4 常用的文件管理方式**

| 文件管理方式 | 应用场景 | 优点 | 缺点 |
|---|---|---|---|
| 直接登录系统 | 通过 Console 口、Telnet 或 STelnet 方式登录设备，对存储器、目录和文件进行管理。特别是对存储器的操作需要通过此种方式 | 对存储器、目录和文件的管理直接通过登录设备完成，方便快捷<br>在通过 Console 本地登录时，可通过 xmodem get 命令从终端向设备传输文件 | Telnet 或 STelnet 方式登录，只能对本设备进行文件操作，无法进行文件传输 |
| FTP | 适用于对网络安全性要求不是很高的文件传输场景中，广泛用于版本升级等业务中 | 配置较简单，支持文件传输及文件目录的操作<br>FTP 可以在两个不同文件系统主机之间传输文件<br>具有授权和认证功能 | 明文传输数据，存在安全隐患 |
| TFTP | 在网络条件良好的实验室局域网中，可以使用 TFTP 进行版本的在线加载和升级。适用于客户端和服务器之间，不需要复杂交互的环境 | TFTP 所占的内存要比 FTP 小 | 设备只支持 TFTP 客户端功能<br>TFTP 只支持文件传输，不支持交互<br>TFTP 没有授权和认证，而且是明文传输数据，存在安全隐患，易于网络病毒传输及被黑客攻击 |
| SFTP | 适用于网络安全性要求高的场景，目前被广泛用于日志下载、配置文件备份等业务中 | 数据进行了严格加密和完整性保护，安全性高<br>支持文件传输及文件目录的操作<br>在设备上可以同时配置 SFTP 功能和普通 FTP 功能。（这一点与 FTPS 方式相比：FTPS 是不可以同时提供 FTPS 和普通 FTP 功能的） | 配置较复杂 |
| SCP | 适用于网络安全性要求高，且文件上传下载效率高的场景 | 数据进行了严格加密和完整性保护，安全性高<br>客户端与服务器连接的同时完成文件的上传下载操作（即连接和拷贝操作使用一条命令完成），效率较高 | 配置较复杂（与 SFTP 方式的配置非常类似），且不支持交互 |

续表

| 文件管理方式 | 应用场景 | 优　点 | 缺　点 |
| --- | --- | --- | --- |
| FTPS | 适用于网络安全性要求高，且不提供普通FTP功能的场景 | 利用数据加密、身份验证和消息完整性验证机制，为基于TCP可靠连接的应用层协议提供安全性保证 | 配置较复杂，需要预先从CA处获得一套证书。若配置FTPS服务，则普通的FTP服务功能必须关闭 |

**7. 配置系统启动**

设备启动时将会启动系统软件和加载配置文件，有效地管理系统软件和配置文件可以保证设备正常启动。其中系统软件是设备启动、运行的必备软件，为整个设备提供支撑、管理、业务等功能，配置文件是命令行的集合。

用户可以进行保存配置文件、比较配置文件、备份配置文件、恢复及清除配置文件等操作。

配置系统启动文件包括指定系统启动用的系统软件和配置文件，这样可以保证设备在下一次启动时以指定的系统软件启动及以指定的配置文件初始化配置。如果系统启动时还需要加载新的补丁，则还需指定补丁文件。

## 3.3　交换机的MAC表

### 3.3.1　MAC地址

MAC(Media Access Control)地址用来定义网络设备的位置。MAC地址由48比特长、12位的十六进制数字组成，0～23位是厂商向IETF等机构申请用来标识厂商的代码，24～47位由厂商自行分派，是各个厂商制造的所有网卡的一个唯一编号。

MAC地址可以分为三种类型。

物理MAC地址：这种类型的MAC地址唯一地标识了以太网上的一个终端，该地址为全球唯一的硬件地址；

广播MAC地址：全1的MAC地址为广播地址(FF-FF-FF-FF-FF-FF)，用来表示LAN上的所有终端设备；

组播MAC地址：除广播地址外，第8b为1的MAC地址为组播MAC地址(例如01-00-00-00-00-00)，用来代表LAN上的一组终端。

### 3.3.2　MAC地址表

设备内有一张MAC地址表，简称MAC表。MAC表记录了相连设备的MAC地址、接口号以及所属的VLAN ID之间的对应关系。在转发数据时，路由设备根据报文中的目的MAC地址和VLAN ID查询MAC地址表，快速定位出接口，从而减少广播。

### 3.3.3 MAC 地址表转发

设备在转发报文时，根据 MAC 地址表项信息，会采取以下两种转发方式。

单播方式：当 MAC 地址表中包含与报文目的 MAC 地址对应的表项时，设备直接将报文向该表项中的转发接口发送。

广播方式：当设备收到的报文为广播报文、组播报文或 MAC 地址表中没有包含对应报文目的 MAC 地址的表项时，设备将采取广播方式将报文向除接收接口外同一 VLAN 内的所有接口转发。

### 3.3.4 MAC 地址表分类

MAC 地址表项分为：动态表项、静态表项和黑洞表项。

动态表项由接口通过源 MAC 地址学习获得，表项有老化时间。为适应网络的变化，MAC 表需要不断更新。MAC 表中自动生成的表项（即动态表项）并非永远有效，每一条表项都有一个生存周期，到达生存周期仍得不到刷新的表项将被删除，这个生存周期被称做老化时间。如果在到达生存周期前记录被刷新，则该表项的老化时间重新计算。

静态表项由用户手工配置，并下发到各接口板，表项不老化。

黑洞表项用于指示丢弃含有特定源 MAC 地址或目的 MAC 地址的数据帧，由用户手工配置，并下发到各接口板，表项不老化。

在系统复位、接口板热插拔或接口板复位后，动态表项会丢失，而保存的静态表项和黑洞表项不会丢失。

## 3.4 交换机的 VLAN 技术

### 3.4.1 VLAN 的定义

VLAN（Virtual Local Area Network）即虚拟局域网，是将一个物理的 LAN 在逻辑上划分成多个广播域的通信技术。VLAN 内的主机间可以直接通信，而 VLAN 间不能直接互通，从而将广播报文限制在一个 VLAN 内。

### 3.4.2 VLAN 的目的

以太网是一种基于 CSMA/CD（Carrier Sense Multiple Access/Collision Detection）的共享通信介质的数据网络通信技术。当主机数目较多时会导致冲突严重、广播泛滥、性能显著下降甚至造成网络不可用等问题。通过交换机实现 LAN 互联虽然可以解决冲突严重的问题，但仍然不能隔离广播报文和提升网络质量。

在这种情况下出现了 VLAN 技术，这种技术可以把一个 LAN 划分成多个逻辑的 VLAN，每个 VLAN 是一个广播域，VLAN 内的主机间通信就和在一个 LAN 内一样，而 VLAN 间则不能直接互通，这样，广播报文就被限制在一个 VLAN 内。

### 3.4.3　VLAN 的作用

限制广播域：广播域被限制在一个 VLAN 内，节省了带宽，提高了网络处理能力。

增强局域网的安全性：不同 VLAN 内的报文在传输时是相互隔离的，即一个 VLAN 内的用户不能和其他 VLAN 内的用户直接通信。

提高了网络的健壮性：故障被限制在一个 VLAN 内，本 VLAN 内的故障不会影响其他 VLAN 的正常工作。

灵活构建虚拟工作组：用 VLAN 可以划分不同的用户到不同的工作组，同一工作组的用户也不必局限于某一固定的物理范围，网络构建和维护更方便灵活。

### 3.4.4　VLAN 的帧格式

VLAN 帧格式对传统的 Ethernet 帧格式进行了修改，在源 MAC 地址字段和协议类型字段之间加入 4 个字节的 802.1Q Tag，如图 3-9 所示。

| 字节长度 | 6 | 6 | 4 | 2 | 46~1500 | 4 |
|---|---|---|---|---|---|---|
| 内容 | 目的地址 | 源地址 | 802.1Q Tag | 类型 | 数据 | FCS |

图 3-9　VLAN 帧格式

其中，802.1Q Tag 包含 4 个字段，各字段解释如表 3-5 所示。

**表 3-5　802.1Q Tag 各字段含义**

| 字段 | 长度 | 名　　称 | 解　　释 |
|---|---|---|---|
| TPID | 2B | Tag Protocol Identifier（标签协议标识符），表示帧类型 | 取值为 0x8100 时表示 802.1Q Tag 帧<br>如果不支持 802.1Q 的设备收到这样的帧，会将其丢弃 |
| PRI | 3b | Priority，表示帧的优先级 | 取值范围为 0～7，值越大优先级越高<br>用于当交换机阻塞时，优先发送优先级高的数据帧 |
| CFI | 1b | Canonical Format Indicator（标准格式指示位），表示 MAC 地址是否是经典格式 | CFI 为 0 说明是经典格式，CFI 为 1 表示为非经典格式。用于兼容以太网和令牌环网。在以太网中，CFI 的值为 0 |
| VID | 12b | VLAN ID，表示该帧所属的 VLAN | VLAN ID 的取值范围是 0～4095。由于 0 和 4095 为协议保留取值，所以 VLAN ID 的有效取值范围是 1～4094 |

每台支持 802.1Q 协议的交换机发送的数据包都会包含 VLAN ID，以指明交换机属于哪一个 VLAN。因此，在一个 VLAN 交换网络中，以太网帧有两种形式：有标记帧（Tagged Frame）即加入了 4 字节 802.1Q Tag 的帧和无标记帧（Untagged Frame），即原始的、未加入 4 字节 802.1Q Tag 的帧。

### 3.4.5 VLAN 链路类型

VLAN 中有以下两种链路类型。

接入链路(Access Link)：用于连接用户主机和交换机的链路。通常情况下，主机并不需要知道自己属于哪个 VLAN，主机硬件通常也不能识别带有 VLAN 标记的帧，主机发出的是 untagged 报文。因此，主机发送和接收的帧都是 untagged 帧。

干道链路(Trunk Link)：用于交换机间的互连或交换机与路由器之间的连接。干道链路可以承载多个不同的 VLAN 数据，数据帧在干道链路传输时，干道链路的两端设备需要能够识别数据帧属于哪个 VLAN，所以在干道链路上传输的帧都是 Tagged 帧。

### 3.4.6 VLAN 接口类型

根据对 VLAN 帧的识别情况，将接口分为 4 类。

**1. Access 接口**

Access 接口是交换机上用来连接用户主机的接口，它只能连接接入链路。仅仅允许唯一的 VLAN ID 通过本接口，这个 VLAN ID 与接口的缺省 VLAN ID 相同，Access 接口发往对端设备的以太网帧永远是不带标签的帧。

**2. Trunk 接口**

Trunk 接口是交换机上用来和其他交换机连接的接口，它只能连接干道链路，允许多个 VLAN 的帧(带 Tag 标记)通过。

**3. Hybrid 接口**

Hybrid 接口是交换机上既可以连接用户主机，又可以连接其他交换机的接口。Hybrid 接口既可以连接接入链路又可以连接干道链路。Hybrid 接口允许多个 VLAN 的帧通过，并可以在出接口方向将某些 VLAN 帧的 Tag 剥掉。

**4. QinQ 接口**

QinQ(802.1Q-in-802.1Q)接口是使用 QinQ 协议的接口。QinQ 接口可以给帧加上双重 Tag，即在原来 Tag 的基础上，给帧加上一个新的 Tag，从而可以支持多达 4094×4094 个 VLAN，满足网络对 VLAN 数量的需求。

### 3.4.7 VLAN 划分

创建并划分 VLAN，将没有互通需求的用户进行隔离，增强网络的安全性、减少广播流量，同时也减少了广播风暴的产生。主要有基于接口划分 VLAN(静态配置链路类型)、基于接口划分 VLAN、基于 MAC 地址划分 VLAN、基于子网划分 VLAN、基于策略划分 VLAN 等方式。

缺省情况下，缺省 VLAN 是 VLAN 1。

一般步骤为需要先创建 VLAN、配置接口的类型，然后将 VLAN 和接口关联。以国产锐捷 RG-S2928G 交换机为例，简单做以下介绍。

操作步骤如下：

(1) 执行命令 enable，从用户模式切换到用户模式。

(2) 通过执行 configure terminal 进入全局配置模式。

(3) 执行命令 vlan vlan-id，创建 VLAN 并进入 VLAN 配置模式。

(4) 执行命令 exit，返回全局配置模式。

(5) 配置以太网接口属性。

缺省情况下，接口的链路类型是 access，且隶属于 VLAN 1。

执行命令 interface interface-type interface-number，进入需要加入 VLAN 的以太网接口配置模式。

执行命令 switchport link-type vlan vlan id，配置以太网接口的链路类型及所属 VLAN。

access、trunk、hybrid 等几种类型，如果以太网接口直接与终端连接，该接口类型一般是 access 类型或 hybrid。

如果以太网接口与另一台交换机设备的接口连接，该接口类型可以是 trunk 类型，也可使用 hybrid。

### 3.4.8　VLAN 配置示例

如图 3-10 所示的网络中(锐捷 RG-S2928G 交换机)，Switch 交换机连接了三个 PC 用户。做 PC1 与 PC3 能互访，且和 PC2 不同属于一个 VLAN 的简单配置。

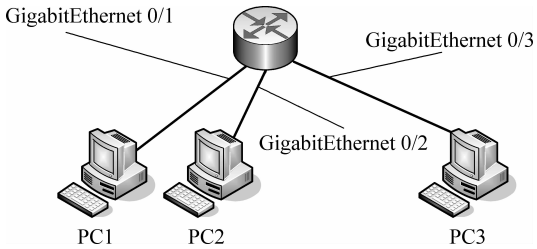


图 3-10　简单 VLAN 划分示例

```
Ruijie>enable                                          * 进入特权模式
Ruijie#configure terminal                              * 进入全局配置模式
Ruijie(config-vlan)#vlan 10
Ruijie(config-vlan)#vlan 20
Ruijie(config)#exit
Ruijie(config)#interface gigabitEthernet 0/1           * 进入接口配置模式
Ruijie(config-if-GigabitEthernet 0/1)#switchport access vlan 10
Ruijie(config-if-GigabitEthernet 0/1)#interface gigabitEthernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)#switchport access vlan 10
Ruijie(config-if-GigabitEthernet 0/3)#interface gigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)#switchport access vlan 20
```

```
Ruijie(config-if-GigabitEthernet 0/2)#end          * 退出接口模式
Ruijie #show running-config                        * 显示配置检查结果
```

### 3.4.9 配置聚合 VLAN

Super VLAN：Super VLAN 是 VLAN 划分的一种方式。Super VLAN 又称为 VLAN 聚合，是一种专门优化 IP 地址的管理技术。其原理是将一个网段的 IP 分给不同的子 VLAN(Sub VLAN)，这些 Sub VLAN 同属于一个 Super VLAN。而每一个 Sub VLAN 都是独立的广播域，不同 Sub VLAN 之间两层相互隔离。当 Sub VLAN 内的用户需要进行三层通信时，将使用 Super VLAN 虚接口的 IP 地址作为网关地址，这样多个 VLAN 共享一个 IP 地址，从而节省了 IP 地址资源。同时，为了实现不同 Sub VLAN 间的三层互通及 Sub VLAN 与其他网络的互通，需要利用 ARP 代理功能。通过 ARP 代理可以进行 ARP 请求和响应报文的转发与处理，从而实现了两层隔离端口间的三层互通。缺省状态下，Super VLAN 和 Sub VLAN 的 ARP 代理功能是打开的。采用 Super VLAN 技术可以极大地节省 IP 地址，它只需对包含多个 Sub VLAN 的 Super VLAN 分配一个 IP 地址，既节省地址又方便网络管理。

**1. 创建 Sub-VLAN**

在 VLAN 聚合中，Sub-VLAN 可以加入物理接口，一般在二层交换机上配置普通 VLAN 即可。

**2. 创建 Super-VLAN**

Super-VLAN 由多个 Sub-VLAN 组成，不能加入物理接口，但可以创建 VLANIF 接口并配置 IP 地址。一般需要在三层交换机上实现。

操作步骤，以锐捷 RG-S5750 交换机为例。

(1) 执行命令 enable，从用户模式切换到用户模式。

(2) 通过执行 configure terminal 进入全局配置模式。

(3) 执行命令 vlan vlan-id，创建 VLAN 并进入 VLAN 视图。本配置步骤中的 vlan-id 与 Sub-VLAN 中的 vlan-id 必须使用不同的 VLAN ID。

(4) 执行命令 supervlan。

(5) 执行命令 subvlan，将 Sub-VLAN 加入 Super-VLAN。将 Sub-VLAN 加入 Super-VLAN 中时，必须保证 Sub-VLAN 没有创建对应的 VLANIF 接口。

### 3.4.10 配置聚合 VLAN 示例

如图 3-11 所示(锐捷 RG-S5750 交换机)，核心交换机 Switch A 作为用户网关设备，通过 Trunk 口连接设备 Switch B、Switch C、Switch D。要求接入用户通过划分 VLAN 实现两层隔离，所有 VLAN 用户共享一个 IP 网关，实现三层通信及与外网通信。

核心交换机 Switch A 配置如下：

(1) 创建 VLAN 2、VLAN 10、VLAN 20、VLAN 30。

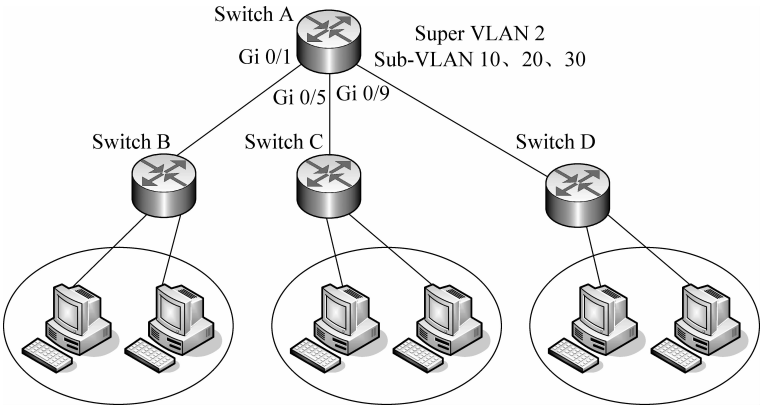


图 3-11　VLAN 聚合示例

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#vlan 2
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 10
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 20
Ruijie(config-vlan)#exit
Ruijie(config)#vlan 30
Ruijie(config-vlan)#exit
```

(2) 设置 VLAN 2 为 Super VLAN，对应的 Sub-VLAN 为 VLAN 10、VLAN 20、VLAN 30。

```
Ruijie(config)#vlan 2
Ruijie(config-vlan)#supervlan                  * 设置 VLAN2 为 Super VLAN
Ruijie(config-vlan)#subvlan 10,20,30           * 管理 subvlan 10、20、30
Ruijie(config-vlan)#exit
```

## 3.5　交换机的生成树技术

### 3.5.1　生成树协议概述

生成树协议(Spanning Tree Protocol，STP)是一个用于在局域网中消除环路的协议。以太网交换网络中为了进行链路备份，提高网络可靠性，通常会使用冗余链路。但是使用冗余链路会在交换网络上产生环路，引发广播风暴以及 MAC 地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为解决交换网络中的环路问题，提出了生成树协议(STP)。

运行 STP 的设备通过彼此交互信息发现网络中的环路，并有选择地对某个端口进行