

---

## 第 3 章 交换机基础

### 本章学习目标

本章从网桥的产生和工作原理讲起，介绍了交换机的产生和工作原理，同时对交换机的外观、功能、体系结构、主要技术参数等进行描述，最后重点介绍交换机的基本配置和常用配置，让读者对交换机有一个全面的了解，掌握交换机的常用基本配置。

通过本章的学习，读者应该掌握以下内容：

- 了解网桥的工作原理。
- 掌握交换机的工作原理。
- 了解交换机的功能、体系结构和主要技术参数等。
- 掌握交换机的基本配置。
- 掌握交换机的常用配置。

### 3.1 交换机的产生和工作原理

#### 3.1.1 网桥的概念和工作原理

##### 1. 网桥的概念

网桥将两个相似的网络连接起来，并对网络数据的流通进行管理。它工作于数据链路层，不但能扩展网络的距离和范围，而且可提高网络的性能、可靠性和安全性。

##### 2. 网桥的工作原理

网桥（Bridge）工作在 OSI 模型的数据链路层，有时称为“二层设备”，这一点是与中继器和集线器完全不一样的，中继器和集线器工作于物理层，处理的信息单元是比特流，而网桥处理的信息单元是数据链路层的数据帧。

网桥的工作原理如下：

（1）当一个端口接收到帧后，网桥检查该帧的目的地址，然后查找地址表，确定与该地址对应的端口。如果收到帧的端口正是帧目的地址所在的端口，那么网桥就会丢弃这个帧。因为可以认定通过正常的 LAN 传输机制，目标机已经接收过这个帧了。例如，如图 3-1 所示网桥在 1 号端口收到了一个从 MACA 站发往 MACB 的帧。由于地址表显示 MACB 在端口 1 上，并且这一帧正是端口 1 接收的，所以网桥会把这个帧丢弃。如果 MACA 接着向 MACC 发送一帧，网桥会从端口 1 接收这一帧（因为网桥处于混杂模式，它接收所有帧），并在地址表中查看站 MACC。地址表说明目的地址是在端口 2 上。为了使目标站正确地收到该帧，网桥必须把这一帧转发到端口 2。

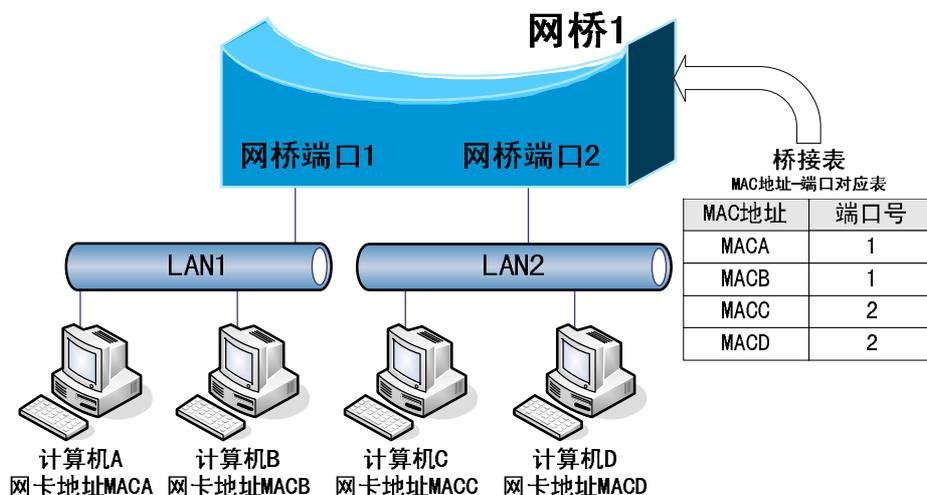


图 3-1 网桥的工作原理

(2) 如果网桥当前还不知道要发送帧的目的地址，网桥在地址表中找不到该目的地址和端口，它便会向除接收该帧之外的所有端口转发此帧，这称为扩散（flooding）或泛洪。扩散使网桥可以与未知的（即在地址表中不存在的）站通信。除了不必要地占用了输出端口的 LAN 带宽以外，帧扩散并没有坏处。如果站真的存在（但此时尚不知道），扩散保证通信能正常进行。与此类似，如果一个站向组播地址发送帧，网桥会向除接收此帧的端口以外的所有端口转发它。这是因为网桥不能确定哪些站正在监听某个组播地址，所以它不应该把帧的转发限制到一个特定的输出端口上。

(3) 通过记录接收帧的源地址，可以动态地建立地址表。当网桥接收到一个帧后，它在表中查找与发送站对应的项（由帧的源地址指明）。如果找到了，就会更新地址表中与该站相对应的端口，以反映在该端口上接收到了最新的帧。这使得网桥可以正确地映射从一个 LAN 网段转移到另一个网段的站。如果没有找到登记项，网桥会根据新发现的地址和接收它的端口地址新建一个新地址表项。经过一段时间，随着站不断地发送帧，网桥就会知道所有活动站的地址—端口对应关系。

因此，网桥有如下特点：

- (1) 在混杂模式下工作。
- (2) 有一个将全局唯一地址映射到网桥端口的地址表。
- (3) 根据所接收帧的目的地址作出转发决定。
- (4) 根据所接收帧的源地址建立和更新地址表。
- (5) 当遇到未知的目的地址时，向每个端口（除接收此帧的端口外）转发该帧。

### 3.1.2 交换机的产生和工作原理

#### 1. 交换机的产生

20 世纪 90 年代初，随着计算机性能的提高及通信量的骤增，传统局域网已经越来越超出了自身的负荷，交换式以太网技术应运而生，大大提高了局域网的性能。与现在基于网桥和路由器的共享媒体的局域网拓扑结构相比，基于交换机的交换式以太网能显著地增加带宽。交换技术的加入，就可以建立地理位置相对分散的网络，使局域网交换机的每个端口可平行、安全、

同时地互相传输信息，而且使局域网可以高度扩充。

交换机的英文名称为 **Switch**，它是在网桥的基础上发展起来的，是集线器的升级换代产品。与集线器不同，交换机之所以能够直接对目的节点发送数据包，而不是像集线器一样以广播方式对所有节点发送数据包，其中最关键的技术就是交换机可以识别连在网络上的节点的网卡 **MAC** 地址，并把它们放到一个叫做 **MAC** 地址表的地方。

## 2. 交换机的工作原理

以太网交换机的原理和网桥的工作原理基本一致，它检测从以太端口来的数据包的源和目的地的 **MAC**（介质访问层）地址，然后与系统内部的动态查找表进行比较，若数据包的 **MAC** 层地址不在查找表中，则将该地址加入查找表，并将数据包发送给相应的目的端口，在这一点上交换机与网桥的工作方式基本一致，如图 3-2 所示。

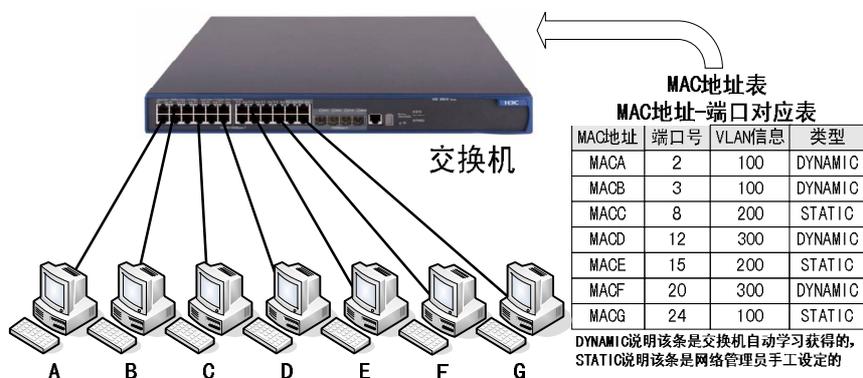


图 3-2 交换机的工作原理

### 3.1.3 交换机、网桥、中继器和集线器的区别

#### 1. 交换机与网桥的区别

(1) 交换机工作时，实际上允许许多组端口间的通道同时工作。所以，交换机的功能体现出不仅仅是一个网桥的功能，而是多个网桥功能的集合。即网桥一般分有两个端口，而交换机具有高密度的端口。

(2) 分段能力的区别。由于交换机能够支持多个端口，因此可以把网络系统划分成更多的物理网段，这样使得整个网络系统具有更高的带宽。而网桥仅仅支持两个端口，所以网桥划分的物理网段是相当有限的。

(3) 传输速率的区别。交换机与网桥数据信息的传输速率相比，交换机要快于网桥。

(4) 数据帧转发方式的区别。网桥在发送数据帧前，通常要接收到完整的数据帧并执行帧检测序列 **FCS** 后才开始转发该数据帧。而交换机根据不同的交换方式，如存储转发、直通、碎片隔离等不同的帧转发方式，可做帧校验，也可以不做帧校验。

(5) 学习 **MAC** 地址上的不同。网桥是一种被动学习，也就是网络中的节点如果不通信，网桥就学习不到 **MAC** 地址，而交换机的学习更加主动一些，当交换机刚启动的时候，它内部的 **MAC** 地址表是空的，交换机会向所有的端口广播发送广播帧，而所有存活节点收到广播帧后就会进行回应，交换机这时就可以从回应帧中学习到 **MAC** 地址，并建立 **MAC** 地址与交换机端口的对应关系。

## 2. 交换机与集线器的区别

(1) 在 OSI/RM (OSI 参考模型) 中的工作层次不同。交换机和集线器在 OSI/RM 开放体系模型中对应的层次不同, 集线器是同时工作在第一层 (物理层) 和第二层 (数据链路层), 而交换机至少是工作在第二层, 更高级的交换机可以工作在第三层 (网络层) 和第四层 (传输层)。

(2) 交换机的数据传输方式不同。集线器的数据传输方式是广播方式, 而交换机的数据传输是有目的的, 数据只对目的节点发送, 只是在自己的 MAC 地址表中找不到的情况下第一次使用广播方式发送, 然后因为交换机具有 MAC 地址学习功能, 第二次以后就不再是广播发送了, 又是有目的地发送。这样的好处是数据传输效率提高, 在安全性方面也不会出现其他节点侦听的现象。

(3) 带宽占用方式不同。在带宽占用方面, 集线器所有端口是共享集线器的总带宽, 而交换机的每个端口都具有自己的带宽, 这样交换机实际上每个端口的带宽比集线器端口可用带宽要高许多, 也就决定了交换机的传输速度比集线器要快许多。换句话说, 如果购买一台 100M 集线器, 这个 100M 是指集线器的背板总线带宽, 而如果购买一台 100M 交换机, 这个 100M 是指交换机的每个端口都可以提供 100M 带宽。

(4) 传输模式不同。集线器只能采用半双工方式进行传输, 因为集线器是共享传输介质的, 这样在上行通道上集线器一次只能传输一个任务, 要么是接收数据, 要么是发送数据。而交换机则不同, 它是采用全双工方式来传输数据, 因此在同一时刻可以同时数据进行接收和发送, 这不但令数据的传输速度大大加快, 而且在整个系统的吞吐量方面交换机比集线器至少要快一倍以上, 因为它可以接收和发送同时进行, 实际上还远不止一倍, 因为端口带宽一般来说交换机比集线器也要宽许多倍。

## 3.2 交换机的概述

### 3.2.1 交换机的外观和产品说明

#### 1. 产品外观

以 H3C 公司的产品为例, 产品外观如图 3-3 所示。



图 3-3 H3C S3610 系列交换机

#### 2. 产品说明

H3C S3610 系列交换机硬件支持 IPv4/IPv6 双栈和 IPv6 over IPv4 隧道 (包括手工 Tunnel、6to4 Tunnel、ISATAP Tunnel、auto-Tunnel)、三层线速转发, 既可以用于纯 IPv4 或 IPv6 网络, 也可以用于 IPv4 到 IPv6 共存的网络, 组网方式灵活, 充分满足当前园区网从 IPv4 向 IPv6 过渡的需求。

支持丰富的 IPv6 路由协议, 包括 RIPng、OSPFv3、ISISv6、BGP4+ for IPv6; 支持 IPv6

的邻居发现协议（Neighbor Discovery Protocol, NDP），管理邻居节点的交互；支持 PMTU 发现（Path MTU Discovery）机制，可以找到从源端到目的端的路径上一个合适的 MTU 值，以便有效地利用网络资源并得到最佳的吞吐量。

H3C S3610 系列多协议交换机目前包含的型号为：

- S3610-28P：24 个 10/100Base-TX 以太网端口，4 个 1000Base-X SFP 千兆以太网端口。
- S3610-28TP：24 个 10/100Base-TX 以太网端口，2 个 1000Base-X SFP 千兆以太网端口，2 个 10/100/1000Base-T 以太网端口。
- S3610-52P：48 个 10/100Base-TX 以太网端口，4 个 1000Base-X SFP 千兆以太网端口。
- S3610-28F：24 个 100Base-X SFP 百兆以太网端口，2 个 1000Base-X SFP 千兆以太网端口，2 个 10/100/1000Base-T 以太网端口。

### 3.2.2 交换机的功能概述

（1）地址学习。交换机能够学习到所有连接到其端口的设备的 MAC 地址。地址学习的过程是通过监听所有流入的数据帧，对其源 MAC 地址进行检验，形成一个 MAC 地址到其相应端口的映射，并将此映射存放在交换机缓存中的 MAC 地址表中。

（2）帧的转发和过滤。当一个数据帧到达交换机后，交换机首先通过查找 MAC 地址表来决定如何转发该数据帧。如果目的地址在 MAC 地址表中有映射时，它被转发到连接目的节点的端口，否则将数据帧向除源端口以外的所有端口转发（如该数据帧为广播帧，则转发至所有端口）。

（3）消除桥接环路。当交换机之间存在有冗余的桥接环路时，交换机通过生成树协议（STP, Spanning Tree Protocol）避免回路的产生，防止数据帧在网络中不断兜圈子的现象发生，同时允许存在后备路径。

（4）不同类型网络的互联。交换机除了能够连接同种类型的网络之外，还可以在不同类型的网络（如以太网和快速以太网之间、以太网和令牌环网之间）之间起到互连作用。如今许多交换机都能够提供支持快速以太网或 FDDI 等的高速连接端口，用于连接网络中的其他交换机或者为带宽占用量大的关键服务器提供附加带宽。

（5）隔离数据流量和网络中发生的故障，这样就可以减少每个网络网段的数据信息流量而使每个网络更有效，提高整个网络效率。

（6）流量控制技术，把流经端口的异常流量限制在一定的范围内。许多交换机具有基于端口的流量控制功能，能够实现风暴控制、端口保护和端口安全。流量控制功能用于交换机与交换机之间在发生拥塞时通知对方暂时停止发送数据包，以避免报文丢失。广播风暴抑制可以限制广播流量的大小，对超过设定值的广播流量进行丢弃处理。

（7）访问控制列表（ACL）技术。ACL 通过对网络资源进行访问输入和输出控制，确保网络设备不被非法访问或被用作攻击跳板。ACL 是一张规则表，交换机按照顺序执行这些规则，并且处理每一个进入端口的数据包。每条规则根据数据包的属性（如源地址、目的地址和协议）要么允许，要么拒绝数据包通过。由于规则是按照一定顺序处理的，因此每条规则的相对位置对于确定允许和不允许什么样的数据包通过网络至关重要。

### 3.2.3 交换机的体系结构

#### 1. 硬件组成

（1）主板（背板）。提供各个业务接口和数据转发单元的联系通道；背板交换容量的大

小直接决定了交换机的最大交换量，这是交换机性能的一个重要指标。

(2) CPU (处理器)。交换机运算的核心部件，它的主频决定了交换机的运算速度，用时间单位内能够完成的计算量来衡量。

(3) RAM (内存)。为 CPU 运算提供动态存储空间，内存空间的大小与 CPU 的主频共同决定了计算机的最大运算量。

(4) Flash。提供永久存储功能，主要保存配置文件和系统文件；Flash 能够快速恢复业务，有效地保证了交换机的正常运转，同时还为网络设备的升级维护提供方便、快捷的方式，如使用 FTP、TFTP 升级或配置等。

(5) 电源系统。为交换机提供电源输入，交换机能否正常运转很大程度上取决于电源系统的性能，输入电压的可变化范围和最大输出电流等是电源系统的重要指标。

## 2. 软件系统

以 H3C 为例，交换机的软件组成主要有以下两部分：

(1) BOOT ROM：主要功能是路由器加电后完成有关初始化工作，并向内存中加入操作系统代码。

(2) COMWARE：是负责系统运行、数据转发的主体软件。

### 3.2.4 交换机的主要技术参数

#### 1. 转发技术

转发技术是指交换机所采用的用于决定如何转发数据包的转发机制。各种转发技术各有优缺点。

(1) 直通转发技术 (Cut-through)。交换机一旦解读到数据包目的地址，就开始向目的端口发送数据包。通常，交换机在接收到数据包的前 6 个字节时，就已经知道目的地址，从而可以决定向哪个端口转发这个数据包。直通转发技术的优点是转发速度快、减少延时和提高整体吞吐率；缺点是交换机在没有完全接收并检查数据包的正确性之前就已经开始了数据转发，这样在通信质量不高的环境下，交换机会转发所有的完整数据包和错误数据包，这实际上是给整个交换网络带来了许多垃圾通信包，交换机会被误解为发生了广播风暴。总之，直通转发技术适用于网络链路质量较好、错误数据包较少的网络环境。

(2) 存储转发技术 (Store-and-Forward)。存储转发技术要求交换机在接收到全部数据包后再决定如何转发。这样一来，交换机可以在转发之前检查数据包的完整性和正确性。其优点是没有残缺数据包转发，减少了潜在的不必要的数据转发；缺点是转发速度比直接转发技术慢。所以，存储转发技术比较适应于普通链路质量的网络环境。

(3) 碰撞逃避转发技术 (Collision-avoidance)。某些厂商 (3COM) 的交换机还提供这种厂商特定的转发技术。碰撞逃避转发技术通过减少网络错误繁殖，在高转发速率和高正确率之间选择了一个折衷的解决办法。

#### 2. 服务质量

服务质量是交换机的一个重要指标。根据业务性质的不同、重要程度的不同进行数据流的划分，有区别地对待这些数据流，是保障紧急重要业务的重要措施，是发挥网络价值的有效方式。

#### 3. 转发能力

以太网交换机的转发能力决定了网络的交换能力。其转发能力可以以是否支持线速转发、

交换容量和包转发率来衡量。以 S3026 为例，其交换容量为 12Gb/s，包转发率为 6.5Mp/s。

#### 4. 背板带宽

背板带宽是指所有业务板与路由交换引擎之间总的通信带宽，如同高速公路的设计总宽度，道路越宽，车越容易跑得快，例如 S9512 的背板带宽是 1.8T。

#### 5. 单/多 MAC 地址类型

单 MAC 交换机的每一个端口只有一个 MAC 硬件地址，它主要用于连接网络最终用户、网络共享资源等，不能连接集线器或含有多个网络设备的网段。多 MAC 交换机在每一个端口上有足够的存储体记忆多个硬件地址。

#### 6. 延时

交换机延时是指从交换机接收到数据包到开始向目的端口复制数据包之间的时间间隔。有许多因素会影响延时大小，如转发技术等。采用直通转发技术的交换机有固定的延时，因为直通式交换机不管数据包的整体大小，而只根据目的地址来决定转发方向，所以它的延时是固定的，取决于交换机解读数据包前 6 个字节中目的地址的解读速率。采用存储转发技术的交换机由于必须要接收完了完整的数据包才开始转发数据包，所以它的延时与数据包大小有关，数据包大，则延时大；数据包小，则延时小。

#### 7. VLAN 支持

目前基本上所有的以太网交换机都支持 VLAN 技术，但是究竟能支持多少个 VLAN、支持何种方式的 VLAN 仍然是交换机性能的一个考核指标。H3C 系列交换机都支持基于端口的 VLAN，S3026E 支持的 VLAN 数高达 256 个。

#### 8. 管理功能

交换机的管理功能是指交换机如何控制用户访问交换机、用户对交换机的可视程度如何。通常，交换机厂商都提供管理软件或满足第三方管理软件远程管理交换机。一般的交换机满足 SNMP MIB I/MIB II 统计管理功能，而复杂一些的交换机会增加通过内置 RMON 组（mini-RMON）来支持 RMON 主动监视功能。有的交换机还允许外接 RMON 监视可选端口的网络状况。

#### 9. 生成树支持

由于交换机实际上是多端口的透明桥接设备，所以交换机也有桥接设备的固有问题——“拓扑环”问题（Topology Loops）。当某个网段的数据包通过某个桥接设备传输到另一个网段，而返回的数据包通过另一个桥接设备返回源地址。这个现象就叫“拓扑环”。一般来说，交换机采用生成树协议算法让网络中的每一个桥接设备相互知道，自动防止拓扑环现象。交换机通过将检测到的“拓扑环”中的某个端口断开，达到消除“拓扑环”的目的，维持网络中的拓扑树的完整性。在网络设计中，“拓扑环”常被推荐用于关键数据链路的冗余备份链路选择。所以，带有生成树协议支持的交换机可以用于连接网络中关键资源的交换冗余。

另外还有很多技术参数，如广播风暴的抑制、镜像、流控、背板带宽、加载升级、管理、安全特性等。

### 3.3 交换机的分类

目前，交换机大致可以按以下几个大类来分：

- (1) 根据网络覆盖范围划分：局域网交换机和广域网交换机。

(2) 根据传输介质和传输速度划分：以太网交换机、快速以太网交换机、千兆（Gb）以太网交换机、10 千兆（10Gb）以太网交换机、FDDI 交换机、ATM 交换机和令牌环交换机。

(3) 根据交换机应用网络层次划分：企业级交换机、校园网交换机、部门级交换机和工作组交换机、桌机型交换机。

(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。

(5) 根据工作协议层划分：第二层交换机、第三层交换机和第四层交换机（通常所指的交换机均为第二层交换机）。

(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。

(7) 根据网络分层设计来划分：访问层交换机、分布层交换机和核心层交换机。

## 3.4 交换机的基本配置

### 3.4.1 交换机的配置方式

交换机的配置方式大体来说有以下几种：

- 通过 Console 口配置。
- 通过拨号远程配置。
- 通过 Telnet 方式配置。
- 通过哑终端方式配置。
- 通过 FTP 方式传送配置文件。

这里重点介绍通过 Console 口配置和通过 Telnet 方式配置两种配置方式。

#### 1. 通过 Console 口配置

Console 口配置是交换机最基本、最直接的配置方式。当交换机第一次配置时，Console 口配置成为配置的唯一手段，因为其他配置方式都必须在交换机上进行一些初始化配置。操作步骤如下：

(1) 用专用配置电缆将配置用主机通信串口和交换机的 Console 口连接起来，如图 3-4 所示。

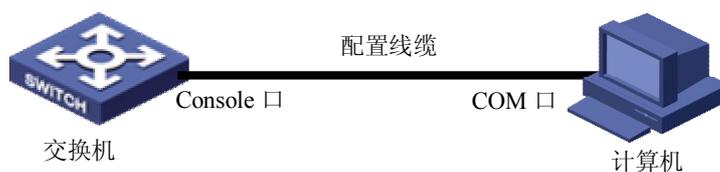


图 3-4 Console 口配置交换机

(2) 启动操作终端，单击“开始”→“所有程序”→“通讯”→“超级终端”命令。

(3) 根据提示输入连接描述名称后单击“确定”按钮（以下配置以 Windows XP 为例），按照图 3-5 至图 3-7 所示操作。

(4) 以太网交换机上电，终端上显示设备自检信息，自检结束后提示用户键入回车，之后将出现命令行提示符（如<H3C>），如图 3-8 所示。



图 3-5 新建连接



图 3-6 连接端口设置



图 3-7 端口通讯参数设置

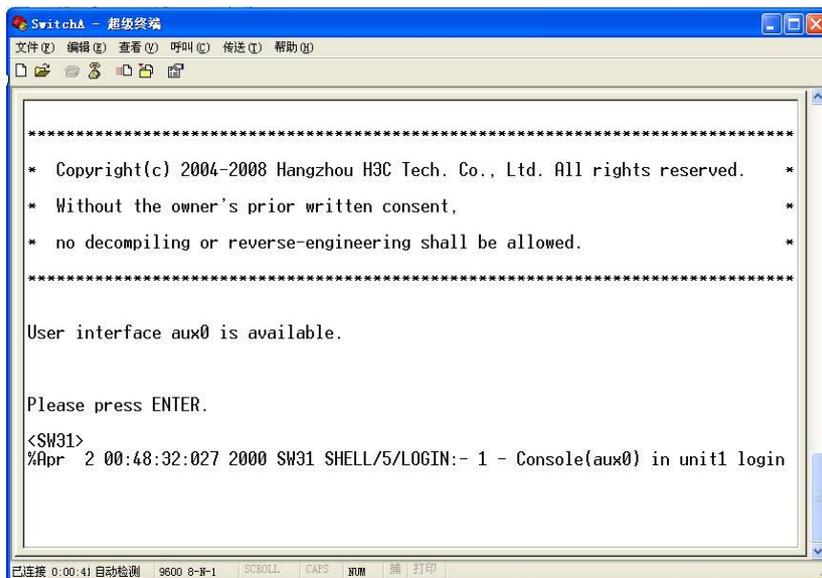


图 3-8 交换机配置界面

(5) 键入命令，配置以太网交换机或查看以太网交换机运行状态。需要帮助可以随时键入“?”，具体的配置命令请参考用户手册中相关部分的内容。

## 2. 通过 Telnet 方式配置

大部分交换机都支持 Telnet 功能，在 Telnet 功能开启的情况下，用户可以通过 Telnet 方式对交换机进行远程管理和维护。这种方式配置的前提是交换机和 Telnet 用户端都要进行相应的配置，以保证通过 Telnet 方式正常登录交换机。主要步骤如下：

(1) 配置交换机的管理 IP 地址，因为要保证交换机和配置用户具有连通性，必须保证交换机具有可与之通信的管理 IP 地址。用 Console 配置方式，在 VLAN 接口视图下配置 IP 地址：

```
<SwitchA>system-view
[SwitchA]interface vlan-interface 1
[SwitchA-Vlan-interface1]ip address 192.168.1.1 24
```

按照图 3-9 所示将交换机和计算机相互连接，并把计算机的 IP 地址设置为 192.168.1.2/24，用 ping 命令测试它们之间的连通性。如果通，则进行下一步。



图 3-9 Telnet 交换机和电脑的连接

(2) 配置用户认证方式。交换机有 3 种认证方式：None（无用户名和密码）、Password（密码）、Scheme（用户名和用户密码），在默认情况下，允许 5 个 vty 用户登录。

- 进入用户界面视图。  
[SwitchA]user-interface vty 0 4
- 配置本地或远端用户名+口令认证方式。  
[SwitchA-ui-vty0-4]authentication-mode scheme
- 配置登录用户的级别为最高级别 3（默认为级别 1）  
[SwitchA-ui-vty0-4]user privilege level 3
- 添加 Telnet 管理的用户，用户类型为 telnet，用户名为 testA，密码为 123456。  
[SwitchA]local-user testA  
[SwitchA-luser-testA]service-type telnet  
[SwitchA-luser-testA]password simple 123456

(3) 通过 Telnet 登录到交换机，登录界面如图 3-10 所示。

注意：

- H3C 交换机最多同时支持 5 个 Telnet 用户登录，如果超过 5 个 Telnet 用户时，交换机将提示“Too many users”，此时请确认 Telnet 用户数量。
- Telnet 登录可以应用 Windows 自带的 DOS、超级终端，也可以应用其他 Telnet 软件进行登录。

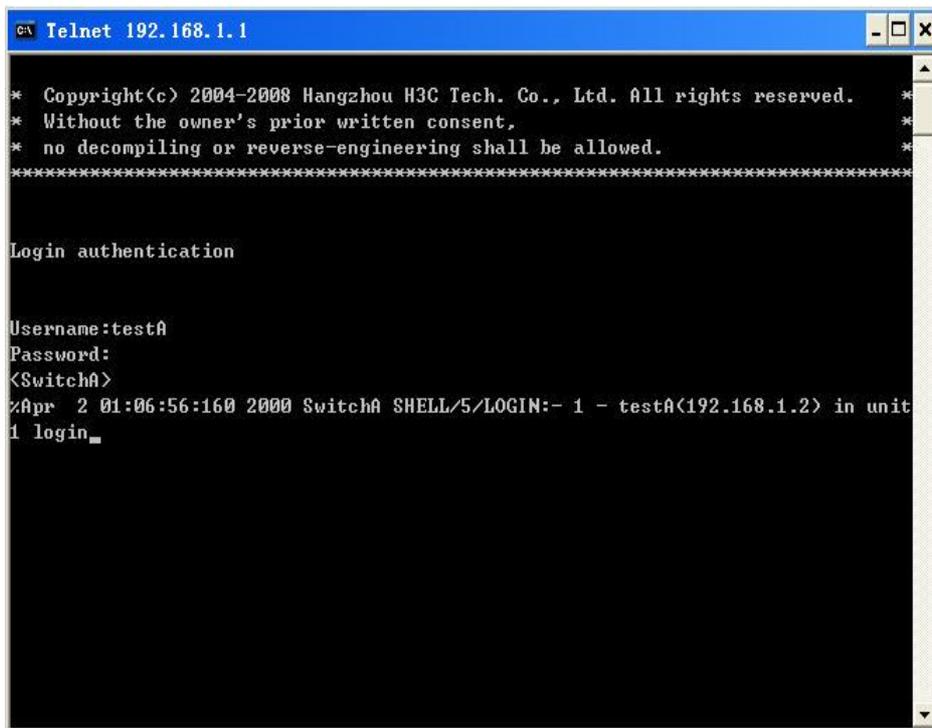


图 3-10 通过 Telnet 登录交换机

### 3.4.2 交换机配置基础

#### 1. 交换机的配置视图

交换机有比较多的视图，各命令行视图是针对不同的配置要求实现的，它们之间既有联系又有区别。比如，用户在与以太网交换机建立连接后即进入用户视图，在用户视图下只能完成查看运行状态和统计信息的简单功能。用户可以键入 `system-view` 进入系统视图，在系统视图下，可以键入不同的命令进入相应的视图。交换机提供的命令行视图以及各命令行视图的功能特性、进入各视图的命令等如表 3-1 所示。

表 3-1 交换机的视图

视图	功能	提示符示例	进入命令	退出命令
用户视图	查看交换机的简单运行状态和统计信息等	<H3C>	与交换机建立连接即进入	quit 断开与交换机的连接
系统视图	配置系统参数	[H3C]	在用户视图下使用 <code>system-view</code> 命令	quit 或 return 返回用户视图
以太网端口视图	配置以太网端口参数	百兆以太网端口视图： [H3C-Ethernet1/0/1]	在系统视图下使用 <code>interface ethernet</code> 命令	quit 返回系统视图 return 返回用户视图
		千兆以太网端口视图： [H3C-GigabitEthernet1/1/1]	在系统视图下使用 <code>interface gigabitethernet</code> 命令	
VLAN 视图	配置 VLAN 参数	[H3C-vlan1]	在系统视图下使用 <code>vlan</code> 命令	

续表

视图	功能	提示符示例	进入命令	退出命令
VLAN 接口视图	配置 VLAN 接口的参数	[H3C-Vlan-interface1]	在系统视图下使用 interface Vlan-interface 命令	
VTY 用户界面视图	配置登录用户的验证参数	[H3C-ui-vty0]	在系统视图下	

进行配置的时候，需要注意配置视图的变化，特定的命令只能在特定的配置视图下执行，否则交换机提示用户输入的是错误的命令或者没有该命令。

**注意：**快捷键 Ctrl+Z 的功能等同于 return 命令。

## 2. 交换机的配置帮助

用户通过在线帮助能够获取到配置过程中所需要的相关帮助信息。命令行接口提供两种在线帮助：完全帮助、部分帮助。

### (1) 完全帮助。

- 在任一视图下，键入“？”，此时用户终端屏幕上会显示该视图下所有的命令及其简单描述。

例如：

```
<SwitchA>?
```

```
User view commands:
```

```
backup      Backup current configuration
boot        Set boot option
cd          Change current directory
clock       Specify the system clock
cluster     Run cluster command
copy        Copy from one file to another
debugging   Enable system debugging functions
delete      Delete a file
dir         List files on a file system
display     Display current system information
fabric      Fabric
fixdisk     Recover lost chains in storage device
format      Format the device
free        Clear user terminal interface
ftp         Open FTP connection
lock        Lock current user terminal interface
mkdir       Create a new directory
```

- 键入一命令，后接以空格分隔的“？”，如果该位置为关键字，此时用户终端屏幕上会列出全部可选关键字及其描述。

例如：

```
<SwitchA> clock ?
```

```
datetime    Specify the time and date
summer-time  Configure summer time
timezone    Configure time zone
```

- 键入一命令，后接以空格分隔的“?”，如果该位置为参数，此时用户终端屏幕上会列出有关的参数描述。键入“?”后，如果只出现<cr>表示该位置无参数，直接键入回车即可执行。

例如：

```
[SwitchA]interface vlan-interface ?
<1-4094> VLAN interface number
```

(2) 部分帮助。

- 键入一字符或一字符串，其后紧接“?”，此时用户终端屏幕上会列出以该字符或字符串开头的命令。

例如：

```
<SwitchA> p?
ping
pwd
```

- 键入命令的某个关键字的前几个字母，按下 Tab 键，如果以输入的字母开头的关键字唯一，用户终端屏幕上会显示出完整的关键字；如果以输入的字母开头的关键字不唯一，反复按下 Tab 键，则终端屏幕依次显示与字母匹配的完整关键字。

### 3. 历史命令

命令行接口提供历史命令记录功能，用户可以通过 `display history-command` 命令随时查看其中已执行过的有效历史命令。默认情况下，命令行接口为每个用户保存 10 条有效历史命令。用户可以按 Ctrl+P 和 Ctrl+N 组合键来查看历史命令。

#### 3.4.3 常用的交换机配置指令

H3C 全系列交换机的命令非常丰富，下面列出一些常用的配置命令。

- `system-view`：进入系统视图模式。
- `sysname`：为设备命名。
- `display current-configuration`：当前配置情况。
- `display saved-configuration`：用来显示 Flash 中以太网交换机的配置文件。
- `save`：用来保存当前配置文件到 Flash 中。
- `reset`：用来擦除 Flash 中以太网交换机的配置文件。
- `language-mode Chinese|English`：中英文切换。
- `interface Ethernet 1/0/1`：进入以太网端口视图。
- `port link-type Access|Trunk|Hybrid`：设置端口访问模式。
- `undo shutdown`：打开以太网端口。
- `shutdown`：关闭以太网端口。
- `quit`：退出当前视图模式。
- `vlan 10`：创建 VLAN 10 并进入 VLAN 10 的视图模式。
- `port access vlan 10`：在端口模式下将当前端口加入到 vlan 10 中。
- `port E1/0/2 to E1/0/5`：在 VLAN 模式下将指定端口加入到当前 vlan 中。
- `port trunk permit vlan all`：允许所有的 vlan 通过。
- `reboot`：用来复位主板，其实就是将交换机重启。

## 3.5 交换机的常用配置

### 3.5.1 交换机文件的上传和下载配置

在交换机中，目前比较流行的方式是用 FTP 服务器上传和下载文件。由于交换机的配置文件可以以文本的方式打开并修改，因此 FTP 也是一种配置交换机的主要方式，而且这种方式和其他方式相比有比较多的优势，能带来意想不到的效果，例如当忘记用户密码时，可以用这种方式重新设置。

以太网交换机可以作为 FTP 服务器，为 FTP 客户端提供文件服务。用户在 PC 上可以运行 FTP 客户端程序登录到 FTP 服务器（即以太网交换机），访问服务器上的文件（接受用户登录前，网络管理员需要事先配置好 FTP 服务器的 IP 地址）。

例子：以太网交换机作为 FTP 服务器，远端的 PC 作为 FTP 客户端。在 FTP 服务器上配置一个 FTP 用户，用户名为 testB，密码为 123456。配置交换机上的一个 VLAN 接口的 IP 地址为 192.168.1.1/24，PC 的 IP 地址为 192.168.1.2/24。交换机和 PC 之间路由可达。交换机的应用程序 SwitchA.bin 保存在 PC 上。PC 通过 FTP 向远端的交换机上传 SwitchA.bin，实现交换机应用程序的升级，同时将交换机的配置文件 Config.cfg 下载到 PC 实现配置文件的备份。按照图 3-9 所示连接好交换机和 PC。

配置步骤如下：

（1）交换机上的配置。

- 用户登录到交换机上（用户可以在本地通过 Console 口登录到交换机上，也可以通过 Telnet 远程登录到交换机上。各种登录方式请参见 3.4.1 节）。
- 在交换机上开启 FTP 服务，并设置用于登录本机 FTP 服务的用户名和密码。  

```
<SwitchA> system-view
[SwitchA] ftp server enable
[SwitchA] local-user testB
SwitchA-luser-testB] password simple 123456
[SwitchA-luser-testB] service-type ftp
```
- 在 PC 上运行 FTP 客户端程序，与交换机建立 FTP 连接。通过上传操作把交换机的应用程序 SwitchA.bin 上传到交换机的 Flash 根目录下，同时从交换机上下载配置文件 Config.cfg。

（2）客户端的配置，这里以 Windows 系统的命令行窗口工具为例进行说明。

- 进入命令行窗口，并切换至 Switch.bin 文件所在的目录（假设该文件存放在 D:\example>目录下）。
- 使用 ftp 功能访问以太网交换机，并输入用户名 testB、密码 123456 进行登录，进入 FTP 视图。  

```
D:\example> ftp 192.168.1.1
Connected to 192.168.1.1.
220 FTP service ready.
User(192.168.1.1:(none)): testB
331 Password required for testB
```

```

Password:
230 User logged in.
ftp>

```

- 上传 SwitchA.bin 文件。

```

ftp> put SwitchA.bin
200 Port command okay.
150 Opening ASCII mode data connection for switch.bin.
226 Transfer complete.

```
- 下载 Config.cfg 文件。

```

ftp> get Config.cfg
200 Port command okay.
150 Opening ASCII mode data connection for config.cfg.
226 Transfer complete.

```

ftp: 收到 1555 字节, 用时 2.00 seconds 0.78Kbytes/sec.

### 3.5.2 交换机的端口配置

交换机的端口技术是交换机的主要技术指标,也是各厂家相互竞争的重要技术之一。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。H3C 交换机的端口基本配置如表 3-2 所示。

表 3-2 端口基本配置表

操作	命令	说明
设置以太网端口描述字符串	<code>description text</code>	可选,默认情况下,端口没有配置描述字符串
设置以太网端口的双工模式	<code>duplex {auto full half}</code>	可选,默认情况下,端口的双工模式为 auto (自协商)
设置以太网端口的速率	<code>speed {10 100 1000 auto}</code>	可选,默认情况下,端口的速率处于 auto (自协商) 状态,仅千兆端口支持配置速率为 1000 Mb/s
设置以太网端口的 MDI (Medium Dependent Interface) 模式	<code>mdi {across auto normal}</code>	可选,默认情况下,端口的 MDI 模式为 auto
设置以太网端口的流量控制功能	<code>Flow-control</code>	默认情况下,禁用了流量控制功能

**注意:** 以上命令均是在交换机的以太网端口视图下配置的。

下面介绍一下目前主要的端口技术。

(1) 端口速率。局域网的发展经历了标准以太网、快速以太网、千兆以太网几个阶段,新阶段所使用的技术都有兼容老一代技术的特点,它们的速度分别是 10M、100M、1000M,交换机的端口速率同样经历了由 10M 到 1000M 的发展,而且快速以太网交换机和千兆以太网交换机的端口速率还可以工作在自适应方式下。

在实际的使用过程中,快速以太网交换机和千兆以太网交换机都支持几种端口速率,那么它们到底是如何与对端通信的呢? H3C 系列交换机有两种工作模式:手工配置和自适应,

默认情况下，所有端口都工作在自适应模式下，通过相互交换自协商报文进行速率的匹配，匹配情况如表 3-3 所示。

表 3-3 端口速率协商表

单位：Mb/s

	标准以太网	快速以太网	千兆以太网
标准以太网	10	10	10
快速以太网	10	100	100
千兆以太网	10	100	1000

当链路两端一端为自协商，另一端为固定速率时，建议修改两端的速率，以保持两端速率的一致性。

(2) 端口工作模式。数据通信中，数据在线路上的传送方式可以分为单工通信、半双工通信和全双工通信三种。为了和网络技术接轨，以太网交换机既支持半双工通信，也支持全双工通信。在实际运用当中，可以人工设置通信的模式，也可以让交换机自行协商通信的模式。

如果交换机自行协商通信的模式，和端口速率协商是一样的，也是通过交换协商报文来协商端口的工作模式，实际上端口模式和端口速率的自协商报文是同一个协商报文。

在端口模式选择过程中要注意以下几点：

- 以太网口的两端工作模式（10M 半双工、10M 全双工、100M 半双工、100M 全双工、自协商）必须设置一致。
- 如果一端是固定模式（无论是 10M 还是 100M），另一端是自协商模式，即便能够协商成功，自协商的那一端也将只能工作在半双工模式。
- 如果一端工作在全双工模式，另一端工作在半双工模式（包括自协商出来的半双工，也一样处理），ping 是没有问题的，流量小的时候没有任何问题，流量达到约 15% 以上时，就会出现冲突、错包，最终影响了工作性能。
- 对于两端工作模式都是自协商，最后协商成的结果是“两端都支持的工作模式中优先级最高的那一类”。
- 如果 A 端自协商，B 端设置为 100M 全双工，A 协商为 100M 半双工后，再强制将 B 改为 10M 全双工，A 端也会立即向下协商到 10M 半双工。
- 如果 A 端自协商，B 端设置为 10M 全双工，A 协商为 10M 半双工后，再强制将 B 改为 100M 全双工，会出现协商不成功，连接不上，这个时候，如果插拔一下网线，又会重新协商在 100M 半双工。

在 H3C 系列交换机上的配置命令如表 3-2 所示。

(3) 端口类型。目前交换机支持的接口有：MDI 介质相关接口和 MDI-X 介质非相关接口。华为系列交换机可以智能识别 MDI、MDIX 接口。路由器和 PC 都属于 MDI 接口，以太网交换机提供的都是 MDI-X 接口。当相互级联的两个端口分别为 MDI 端口和 MDI-X 端口时，应当使用直通线；当相互级联的两个端口均为 MDI 或 MDI-X 端口时，则应当使用交叉线。

在实际使用过程中，网络用户往往在决定到底是选择交叉线还是直连线问题上搞混淆，H3C 系列交换机考虑到这种情况，通过新一代的物理层芯片和变压器技术实现了 MDI 和 MDI-X 接口智能识别和转换的功能，不论使用的是直连线还是交叉线都可以与同接口类型或

不同接口类型的以太网设备互通。

当用户需要手工强制确定端口的接口类型时，可以使用配置命令，参见表 3-2。

(4) 端口流量控制。当两台不同设备之间缓冲区的大小或工作效率不同而进行通信时，可能发生数据的丢失。比如发送端（交换机 A）的缓冲区比较大，而接收端（交换机 B）的缓冲区比较小。当交换机 A 将数据源源不断地发送到交换机 B 的过程中，由于交换机 A 的缓冲区比交换机 B 的要大，那么交换机 B 的缓冲区就装不下这么多流量。如果交换机 B 不能很快地释放其缓存区中的数据，那么在交换机 B 中就可能发生缓冲区溢出故障，从而发生数据流量的丢失。

在 IEEE 802.3 中，提出了流量控制的特性。通过这个特性，就可以有效地避免设备之间的流量丢失。这个数据流量控制功能的工作原理比较简单，就是提供了判断两台设备链路缓冲区是否满的手段。当链路伙伴发现对端设备的缓冲区已经满了时，则将停止发送数据流量，并且在对端设备表明它具有接收流量的能力之后（缓冲区得到一定的释放之后）再重新发送流量。

H3C 系列交换机都支持这个流量控制特性，实际上，H3C 系列交换机中所有端口默认情况下都禁用了流量控制功能，如果需要开启流量控制功能，则执行表 3-2 中的流量控制命令。

## 习题与思考

1. 思考交换机的工作原理，总结交换机、网桥、中继器、集线器的区别和联系。
2. 交换机的硬件构成和软件构成是什么，有哪些技术参数？
3. 交换机有几种配置方式？思考把交换机作为 FTP 客户机和服务器两种方式去配置交换机的原理和方法。
4. 交换机的视图有哪些，分别有什么配置命令？
5. 交换机的端口配置有哪些需要注意的？自己实验和总结。

---

## 第 4 章 虚拟局域网技术

### 本章学习目标

本章从 VLAN 的产生背景入手，对 VLAN 的划分、VLAN 的帧格式、VLAN 端口类型、VLAN 之间的通信进行详细描述。

通过本章的学习，读者应该掌握以下内容：

- 了解 VLAN 的产生背景。
- 理解 VLAN 的划分。
- 理解 VLAN 的帧格式。
- 掌握端口类型。
- 掌握 VLAN 之间的通信及基本配置。

### 4.1 VLAN 的产生背景

在以太网的发展过程中，传统网络的主要问题是可用性和性能。这两个问题受网络中带宽总和的影响。在一个碰撞域中，数据帧对该局域网上的所有设备都是可见的，因此，广播、多点广播、未知的单点传送数据帧都有可能占用过多的带宽。广播数据流量随着网络的增长而增长。过多的广播会减少最终用户的可用带宽，在最坏的情形下，广播风暴甚至可以使整个网络瘫痪。另一方面，在一个只由网桥构成的网络中，所有连在网上的工作站和服务器都不得不对广播数据帧进行解码，该动作会产生额外的 CPU 中断并降低应用性能。经过不断地使用，后来人们又发现，除了可用性和性能的缺点，传统以太网的安全性差、移动代价高等问题也不断暴露出来。为此，IEEE 协会专门设计规定了 802.1q 协议标准，这就是 VLAN 技术的根本，VLAN 技术由此发展起来。

VLAN (Virtual Local Area Network) 又称虚拟局域网，是指在交换局域网的基础上，采用网络管理软件构建的可跨越不同网段、不同网络的端到端的逻辑网络。一个 VLAN 组成一个逻辑子网，即一个逻辑广播域，它可以覆盖多个网络设备，允许处于不同地理位置的网络用户加入到一个逻辑子网中。

### 4.2 VLAN 的划分

目前，从技术角度讲，VLAN 的划分可依据不同原则，一般有以下几种划分方法：

(1) 基于端口的虚拟局域网。基于端口的虚拟局域网是最实用的虚拟局域网，它保持了最普通最常用的虚拟局域网成员定义方法，配置也相当直观简单，局域网中的站点具有相同的网络地址，不同的虚拟局域网之间进行通信需要通过路由器。采用这种方式的虚拟局域网的不足之处是灵活性不好。例如，当一个网络站点从一个端口移动到另外一个新的端口时，如果新

端口与旧端口不属于同一个虚拟局域网，则用户必须对该站点重新进行网络地址配置，否则该站点将无法进行网络通信。在基于端口的虚拟局域网中，每个交换端口可以属于一个或多个虚拟局域网组，比较适用于连接服务器。

(2) 基于 MAC 地址的虚拟局域网。在基于 MAC 地址的虚拟局域网中，交换机对站点的 MAC 地址和交换机端口进行跟踪，在新站点入网时根据需要将其划归至某一个虚拟局域网，而无论该站点在网络中怎样移动，由于其 MAC 地址保持不变，因此用户不需要进行网络地址的重新配置。这种虚拟局域网技术的不足之处是，在站点入网时需要对交换机进行比较复杂的手工配置，以确定该站点属于哪一个虚拟局域网。

(3) 基于 IP 地址的虚拟局域网。在基于 IP 地址的虚拟局域网中，新站点在入网时无须进行太多配置，交换机会根据各站点网络地址自动将其划分成不同的虚拟局域网。在三种虚拟局域网的实现技术中，基于 IP 地址的虚拟局域网智能化程度最高，实现起来也最复杂。

(4) 基于网络层划分 VLAN。根据每个主机的网络层地址或协议类型（如果支持多协议）划分，虽然这种划分方法根据的是网络地址，如 IP 地址，但它不是路由，与网络层的路由毫无关系。在查看每个数据包的 IP 地址时，由于不是路由，所以没有 RIP、OSPF 等路由协议，而是根据生成树算法进行桥交换。这种方法的优点是，一旦用户的物理位置改变，不需要重新配置所属的 VLAN，而且可以根据协议类型来划分 VLAN，这对网络管理者来说很重要；这种方法不需要附加的帧标签来识别 VLAN，这样可以减少网络的通信量。缺点是效率低，因为检查每一个数据包的网路层地址是需要消耗处理时间的（相对于前面两种方法），一般的交换机芯片都可以自动检查网络上数据包的以太网帧头，但要让芯片能检查 IP 帧头，则需要更高的技术，同时也更费时，当然这决定于各个厂商的实现方法。

(5) 根据 IP 组播划分 VLAN。IP 组播实际上也是一种 VLAN 的定义，即认为一个组播组就是一个 VLAN，这种划分的方法将 VLAN 扩大到了广域网，因此这种方法具有更大的灵活性，而且也很容易通过路由器进行扩展，但这种方法不适合局域网，主要是效率不高。

鉴于当前业界 VLAN 发展的趋势，考虑到各种 VLAN 划分方式的优缺点，为了最大程度上满足用户在具体使用过程中的需求，减轻用户在 VLAN 具体使用和维护中的工作量，H3C 系列交换机采用根据端口来划分 VLAN 的方法。

### 4.3 VLAN 的帧格式

IEEE 802.1q 协议标准定义了在同一条物理链路上承载多个子网的数据流的方法，它是一个有关 trunk 封装方式的标准。为了保证不同厂家生产的设备能够顺利互通，IEEE 802.1q 标准严格规定了统一的 VLAN 帧格式以及其他重要参数，它是在原有标准以太网帧格式基础上修订而成的，在以太网数据帧的源 MAC 地址后面增加了 4 字节的 Tag 域（如图 4-1 所示），该域前 2 个字节是标签协议标识（TPID），后 2 个字节为标签控制信息（TCI）。

(1) 目的地址字段 DA (Destination Address): 占 2 个或 6 个字节，用于标识接收站点的地址。它分为单播地址、组播地址和广播地址。表示单播地址时，DA 字段最高位为“0”；表示组播地址时，DA 字段最高位为“1”，其余位不全为“1”，该地址指定网络上给定的多个站点；表示广播地址时，DA 字段全为“1”，该地址指定网络上所有的站点。

(2) 源地址字段 SA (Source Address): 占 2 个或 6 个字节，其长度与目的地址字段的长度相同，它用于标识发送站点的地址。

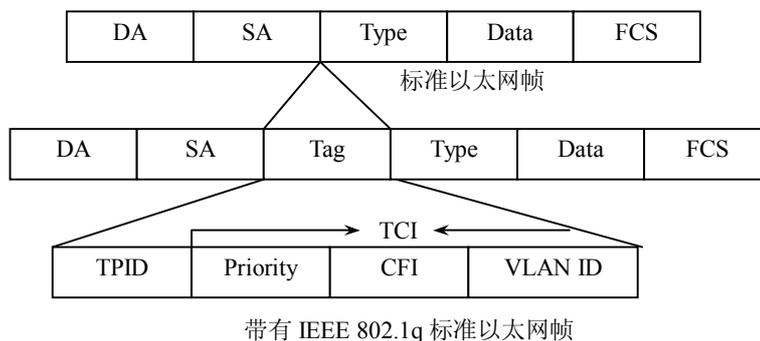


图 4-1 增加的 Tag 域

(3) 标记协议标识 TPID (Tag Protocol Identifier): 占 2 个字节, 该字段固定的值为十六进制 0x8100, 表示这是一个添加了 802.1q 标签的帧。

(4) 标签控制信息 TCI (Tag Control Information): 占 2 个字节, 它包括 3 位用户优先级 UP (User Priority)、1 位规范格式指示器 CFI (Canonical Format Indicator) 和 12 位 VLAN ID。IEEE 802.1q 协议标准中没有定义和使用优先级字段, 而 IEEE 802.1p 中则定义了该字段。

(5) 类型/长度字段 Type/LEN (Type/Length): 占 2 个字节, 其值表示数据字段的字节数长度。如果是采用可选格式组成帧结构时, 该字段既表示包含在帧数据字段中的数据长度, 也表示帧类型 ID。

(6) 数据字段 (Data): 其内容即为 LLC 子层递交的 LLC 帧序列, 其长度为 0~1500 个字节。

(7) 帧校验序列字段 FCS (Frame Check Sequence): 占 4 个字节, 该序列包含 32 位循环冗余校验码 (CRC) 值, 其校验范围不包括前导码字段 P 及帧起始定界符字段 SFD。由发送方生成, 接收方根据此值重新计算可判断并校验被破坏的帧。

## 4.4 VLAN 端口

从交换机所处理的 VLAN 数据帧的不同, 我们可以将交换机的端口分成三类: 第一类是只能传送标准以太网帧的端口, 称为 Access 端口; 第二类是既可以传送有 VLAN 标签的数据帧也能够传送标准以太网帧的端口, 称为 Trunk 端口; 第三类可以灵活传送数据帧, 通过用户的设置可以同时传送带有 VLAN 标签的数据帧和标准以太网帧, 称为 Hybrid 端口。

对于三类端口的一些规定如下:

(1) Access 类型: 端口只能属于一个 VLAN, 一般用于连接计算机。

(2) Trunk 类型: 端口可以属于多个 VLAN, 可以接收和发送多个 VLAN 的报文, 一般用于交换机之间的连接。

(3) Hybrid 类型: 端口可以属于多个 VLAN, 可以接收和发送多个 VLAN 的报文, 可以用于交换机之间的连接, 也可以用于连接用户的计算机。

三种类型的端口可以共存在一台设备上, 但 Trunk 端口和 Hybrid 端口之间不能直接切换, 只能先设为 Access 端口, 再设置为其他类型端口。例如, Trunk 端口不能被设置为 Hybrid

端口，只能先设为 Access 端口，再设置为 Hybrid 端口。H3C 系列 VLAN 端口的配置如表 4-1 所示，配置实例详见 4.6 节。

表 4-1 VLAN 端口的配置

操作	命令	说明
进入以太网端口视图	<code>interface interface-type interface-number</code>	无
配置端口的链路类型	<code>port link-type {access trunk Hybrid}</code>	
设置端口的默认 VLAN ID	<code>Port{Trunk hybrid} pvid vlan vlan-id</code>	Access 端口只能属于一个 VLAN，所以它的默认 VLAN 就是它所在的 VLAN，不用设置。Hybrid 端口和 Trunk 端口可以属于多个 VLAN，所以需要设置端口的默认 VLAN ID
将当前端口加入到指定的 VLAN	<code>port access vlan vlan-id</code> <code>port hybrid vlan vlan-id-list { tagged   untagged }</code> <code>port trunk permit vlan {vlan-id-list   all }</code>	用户可以设置 Hybrid 端口在转发指定的 VLAN 报文时是否保留 VLAN Tag

注意：

- Hybrid 端口可以允许多个 VLAN 的报文发送时不打标签，而 Trunk 端口只允许默认 VLAN 的报文发送时不打标签。
- 建议将本端 Hybrid 端口或 Trunk 端口的默认 VLAN ID 和相连的对端交换机的 Hybrid 端口或 Trunk 端口的默认 VLAN ID 配置为一致，否则端口可能无法正确转发报文。

配置了以太网端口的默认 VLAN ID 后，端口对报文的接收和发送的处理有几种不同情况，具体描述如表 4-2 所示。

表 4-2 端口对收发报文的处理

端口类型	对接收报文的处理		发送报文时的处理
	不带 Tag 时	带有 Tag 时	
Access 端口		当 VLAN ID 与默认 VLAN ID 相同时：接收该报文 当 VLAN ID 与默认 VLAN ID 不同时：丢弃该报文	由于 VLAN ID 就是默认 VLAN ID，不用设置，去掉 Tag 后发送
Trunk 端口	接收该报文，并为报文添加默认 VLAN 的 Tag	当 VLAN ID 与默认 VLAN ID 相同时：接收该报文 当 VLAN ID 与默认 VLAN ID 不同时，但 VLAN ID 是该端口允许通过的 VLAN ID 时：接收该报文	当 VLAN ID 与默认 VLAN ID 相同时：去掉 Tag，发送该报文 当 VLAN ID 与默认 VLAN ID 不同时：保持原有 Tag，发送该报文
Hybrid 端口		当 VLAN ID 与默认 VLAN ID 不同时，且 VLAN ID 是该端口不允许通过的 VLAN ID 时：丢弃该报文	当报文中携带的 VLAN ID 是该端口允许通过的 VLAN ID 时，发送该报文，并可以通过 <code>port hybrid vlan</code> 命令配置端口，在发送该 VLAN（包括默认 VLAN）的报文时是否携带 Tag

## 4.5 VLAN 间路由

通过前面的学习我们已经知道，VLAN 可以控制广播并将数据通信限制在本地，阻止不同 VLAN 之间设备的通信，提高网络的安全性能。VLAN 内部的网络设备的通信通过二层交换机可以实现，那么位于不同 VLAN 的网络设备要进行通信怎么办呢？答案是利用第三层的设备路由器来实现，也称为 VLAN 间路由。

对于目前广泛采用的 TCP/IP 网络，通常每个 VLAN 是一个独立的网段或子网，若不是同一网段则不能解决互通的问题，在配置时绝大多数厂商的交换机需要将不同的 VLAN 配置为不同的网段。

如图 4-2 所示，若 VLAN 2 用户和 VLAN 3 用户在同一网段中，它们之间不需要经过路由器，靠第二层广播就可以通信，但是由于分属不同的 VLAN，第二层广播报文被隔离，这样这两个 VLAN 之间就无法通信了，所以通常将不同的 VLAN 用户划分到不同的网段，它们之间的通信可以通过路由方式来实现。

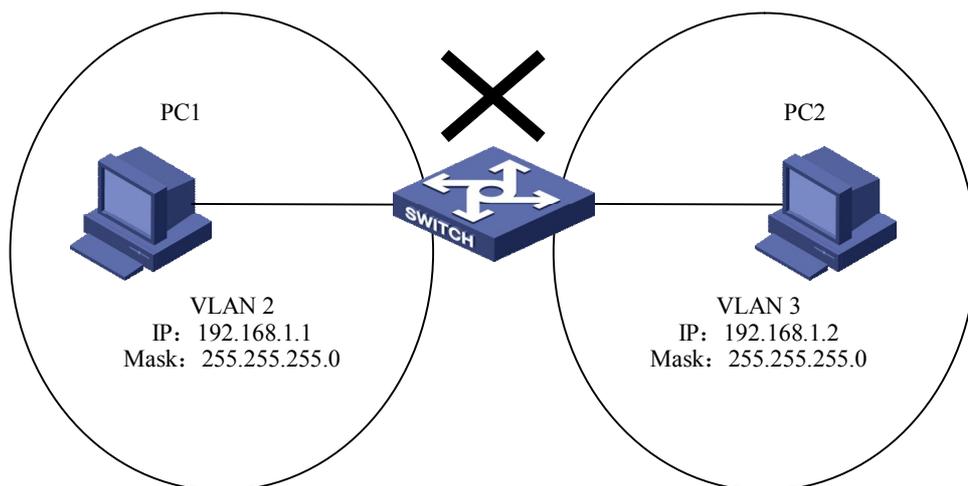


图 4-2 同一网段不同 VLAN 的用户间不能通信

虽然采用路由方式实现了 VLAN 之间的通信，但是采用什么设备又是个问题。如果是具有路由功能的三层交换机当然最好，而且通常把路由器和交换机的功能结合起来，采用“一次路由，多次交换”的方法，即同一 VLAN 间的通信只需要分析首个数据包的 IP 地址信息，进行路由查找等，完成第一个数据包的转发后，三层交换机会在二层建立快速映射，当同一数据包到达时，直接按照快速转发映射进行转发，而不需要每一个数据包都经过路由，极大地提高了转发的速度，优化了性能。

但是许多时候为了节省购买三层交换机的大额投资而使用外部路由器，这时又出现了新的问题。当使用外部路由器时，由于路由器的一个物理接口只能连接一个网段，若使用传统技术，则每个 VLAN 需要一个路由器接口，很不经济，如图 4-3 所示。而且这种方法限制了 VLAN 数量的增加，不利于网络的发展，实际应用显然行不通。

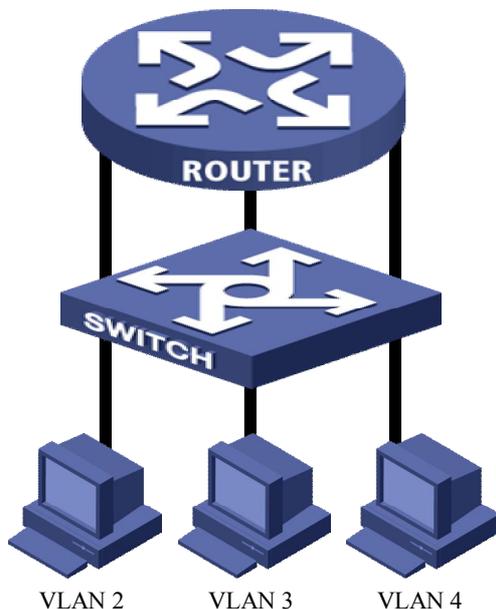


图 4-3 每个 VLAN 一条物理连接

那么能够用外部路由器的一个物理接口把所有 VLAN 都连起来，即用一条物理链路传送所有 VLAN 的数据流呢？回答是肯定的。只要路由器的以太网接口支持 VLAN Trunking 功能，就可以把路由器和交换机的链路设置成 Trunk，传递所有 VLAN 的数据流，再将路由器的这个以太网接口划分成与 VLAN 等数量的子接口，每个子接口连接一个 VLAN，于是问题就解决了，如图 4-4 所示，这种办法称为独臂路由（one-armed-router）。这种办法的缺点是外部路由器与交换机之间的单一链路承担了 VLAN 之间的所有通信量，容易成为交通瓶颈，当 VLAN 间通信量较大时需要较宽的带宽。

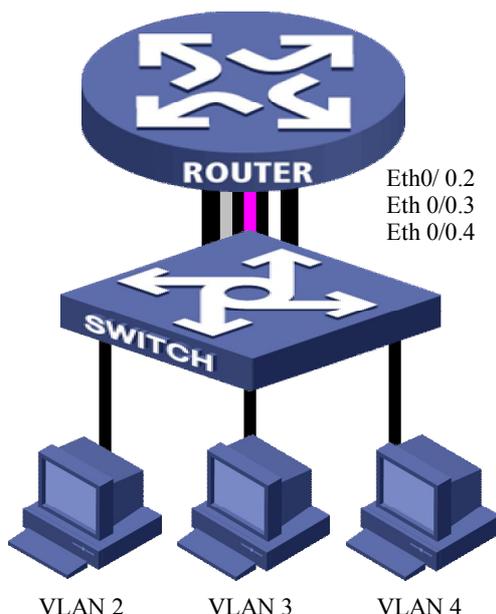


图 4-4 一条物理连接上支持多个 VLAN

## 4.6 VLAN 配置

前面讲过交换机的端口配置、VLAN 端口类型等基础知识，现在结合前面的知识来配置 VLAN（基于端口的 VLAN）。

### 4.6.1 VLAN 的基本配置

交换机的 VLAN 基本配置包括创建 VLAN 和向当前 VLAN 添加端口，命令如表 4-3 所示。

表 4-3 VLAN 的基本配置

操作	命令	说明
创建 VLAN 并进入 VLAN 视图	<code>vlan <i>vlan-id</i></code>	<code>vlan-id</code> 的取值范围为 1~4094
指定当前 VLAN 的名称	<code>name <i>text</i></code>	默认情况下，VLAN 的名称为该 VLAN 的 VLAN ID
指定当前 VLAN 的描述字符串	<code>description <i>text</i></code>	默认情况下，VLAN 的描述字符串为该 VLAN 的 VLAN ID
向 VLAN 中添加端口	<code>port <i>interface-list</i></code>	默认情况下，所有端口都已加入到系统默认的 VLAN 中
显示 VLAN 相关信息	<code>display vlan [<i>vlan-id</i> [to <i>vlan-id</i>]   all   dynamic   static ]</code>	<code>display</code> 命令可以在任意视图下执行

### 4.6.2 VLAN 接口的基本配置

对 VLAN 接口进行配置的前提是首先要创建 VLAN。VLAN 接口的基本配置如表 4-4 所示。

表 4-4 VLAN 接口的基本配置

操作	命令	说明
系统视图下创建 VLAN 接口并进入 VLAN 接口视图	<code>interface vlan-interface <i>vlan-id</i></code>	<code>vlan-id</code> 的取值范围为 1~4094
指定当前 VLAN 接口的描述字符串	<code>description <i>text</i></code>	默认 VLAN 接口的描述字符串为该 VLAN 接口的接口名
打开/关闭 VLAN 接口	<code>[undo]shutdown</code>	
显示 VLAN 接口的相关信息	<code>display interface vlan-interface <i>vlan-id</i></code>	<code>display</code> 命令可以在任意视图下执行

打开/关闭 VLAN 接口的操作对属于该 VLAN 的以太网端口的状态没有影响。VLAN 接口的管理状态默认为打开，此时 VLAN 接口物理状态受 VLAN 中端口状态的影响，即当 VLAN 中所有以太网端口状态为 DOWN 时，VLAN 接口为 DOWN 状态，即关闭状态；当 VLAN 中有一个或一个以上的以太网端口处于 UP 状态时，则 VLAN 接口处于 UP 状态。如果将 VLAN 接口的管理状态设置为关闭，则 VLAN 接口的物理状态始终为 DOWN，不受 VLAN 中端口状态的影响。

### 4.6.3 配置实例

(1) 组网需求。

- 创建 VLAN2、VLAN3，指定 VLAN2 的描述字符串为 home。
- 要求 PCA、PCB、PCC 属于 VLAN2，PCD、PCE、PCF 属于 VLAN3，相同子网能互访，不同子网不能互访。
- PCA、PCB、PCF 分别连接交换机 A 的 Ethernet1/0/1~Ethernet1/0/3，PCC、PCD、PCE 分别连接交换机 B 的 Ethernet1/0/1~Ethernet1/0/3，交换机之间用 Ethernet1/0/4 相连，按照网络拓扑图（如图 4-5 所示）连接好设备。

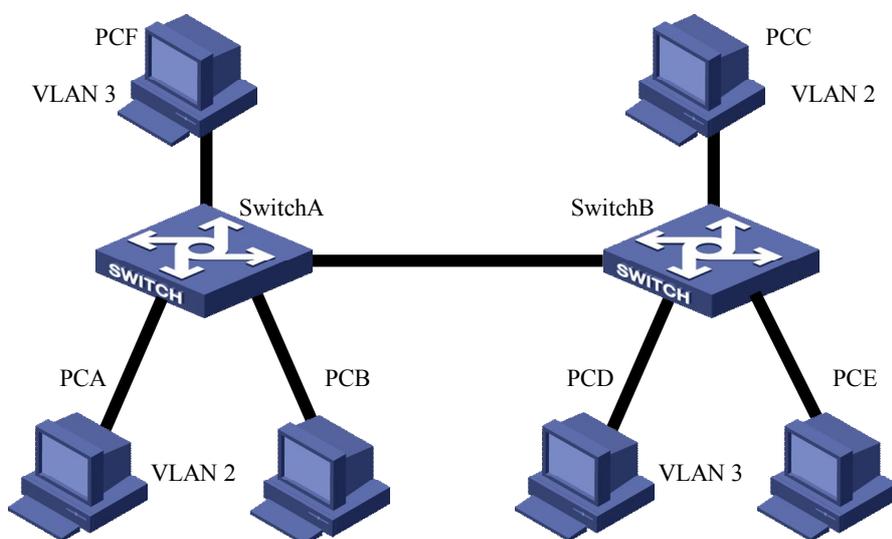


图 4-5 VLAN 配置实例

(2) 配置步骤。

1) SwitchA。

- 创建 VLAN2 并进入其视图。  

```
< SwitchA> system-view
[SwitchA] vlan 2
```
- 指定 VLAN2 的描述字符串为 home。  

```
[SwitchA-vlan2] description home
```
- 向 VLAN2 中加入端口 Ethernet1/0/1 和 Ethernet1/0/2。  

```
[SwitchA-vlan2] port Ethernet 1/0/1 to Ethernet 1/0/2
```
- 创建 VLAN3 并进入其视图。  

```
[SwitchA-vlan2] vlan 3
```
- 向 VLAN3 中加入端口 Ethernet1/0/3。  

```
[SwitchA-vlan3] port Ethernet 1/0/3
```
- 配置端口的类型。  

```
[SwitchA-Ethernet1/0/4]port link-type trunk
```

- 设定 Trunk 端口允许通过 VLAN2 和 VLAN3 的数据。

```
[SwitchA-Ethernet1/0/4]port trunk permit vlan 2 to 3
```

## 2) SwitchB。

- 创建 VLAN2 并进入其视图。

```
< SwitchB> system-view
```

```
[SwitchB] vlan 2
```

- 指定 VLAN2 的描述字符串为 home。

```
[SwitchB-vlan2] description home
```

- 向 VLAN2 中加入端口 Ethernet1/0/1。

```
[SwitchB-vlan2] port Ethernet 1/0/1
```

- 创建 VLAN3 并进入其视图。

```
[SwitchB-vlan2] vlan 3
```

- 向 VLAN3 中加入端口 Ethernet 1/0/2 和 Ethernet1/0/3。

```
[SwitchB-vlan3] port Ethernet 1/0/2 to Ethernet 1/0/3
```

- 配置端口的类型。

```
[SwitchB-Ethernet1/0/4]port link-type trunk
```

- 设定 Trunk 端口允许通过 VLAN2 和 VLAN3 的数据。

```
[SwitchB-Ethernet1/0/4]port trunk permit vlan 2 to 3
```

## 习题与思考

1. 简述 VLAN 的产生背景。
2. VLAN 的划分有几种方式，优缺点分别是什么，最常用的是哪些？
3. VLAN 的帧格式和标准以太网的帧格式有什么异同？
4. 交换机的端口类型有几种，在接收和发送数据包时分别对数据是怎样处理的？