4 Cisco IOS 交换机二层接口配置与管理

在 Cisco IOS 以太局域网交换机上的接口类型，如果从特性来划分主要有 4 种：交换端口（Switch Port）、可路由端口（Routed Port）、交换机虚拟接口（Switch Virtual Interface，SVI）和以太网通道端口组（EtherChannel Port Group，EPG）接口。交换端口就属于二层端口，包括访问端口（Access Port）、中继端口（Trunk Port）和隧道端口（Tunnel Port）3 种类型。另外，有些交换机还有 Uplink 端口、EMP 端口（Ethernet Management Port，以太网管理端口）、PoE 端口（Power over Ethernet Port，PoE）和 USB 接口等，但这些接口类型属于特殊接口，并不是每台交换机上都有。

本章作为正式使用 IOS 系统配置 Cisco 交换机的开篇，首先介绍的是 Cisco IOS 交换机的以太网接口类型、以太网接口的配置与管理，以及二层以太网接口属性的配置与管理，如以太网接口速率、接口双工模式、接口流量控制、MAC 地址列表、链路状态和中继状态事件日志配置与管理等。但在这里要特别注意的是，这些以太网接口二层属性配置以及这里介绍的以太网接口管理方法不仅适用于纯二层以太网接口，同样适用于下一章将要介绍的 IOS 交换机各种三层以太网接口（或者像 SVI、以太网通道等虚拟端口）。

4.1 IOS 交换机上的交换端口及配置与管理

Cisco IOS 交换机的交换端口（Switch Port）是仅与一个物理接口（不能是虚拟端口）关联的二层接口，可属于一个或者多个 VLAN，具体是属于一个还是属于多个 VLAN 要视具体的交换端口类型而定，将在下面介绍具体交换端口类型时介绍。交换端口用来管理物理接口和关联二层协议，不能处理路由和 Fallback Bridging（后退桥接）。**注意，本节的内容相当重要，也比较难懂**。

【说明】Fallback Bridging（后退桥接，也叫 VLAN 桥接）可以使不同的 VLAN 通过可路由端口转发交换机不能路由的非 IP 流量（仅限非 IP 流量），比如 DECnet 协议的流量。在后退桥接中，每个 VLAN 有单独的生成树，通常称之为“VLAN 桥接生成树”，用于防止环路。从上述可以得出，后退桥接是 VLAN 间通过可路由端口的一种相互进行非 IP 访问的解决方案。

在 Cisco 交换机中，交换端口又可划分为：访问端口（Access Port）、中继端口（Trunk Port）、隧道端口（Tunnel Port）3 种。可以配置一个端口作为 Access 端口或 Trunk 端口，也可以在基于每端口基础上运行 DTP（Dynamic Trunking Protocol，动态中继协议），通过与链路另一端的端口协商设置为交换端口模式。但你必须手动配置 Tunnel 端口作为一条连接到 IEEE 802.1Q 隧道的非对称链路的一部分。

可通过使用 **switchport** 接口配置模式命令来把一个当前工作在三层模式的接口转换成二层模式接口；使用 **no switchport** 接口配置模式命令可以把工作在二层模式的接口转换成三层模式。Cisco 交换机上默认所有的以太网接口均属于二层模式。在转换二层模式接口为三层模式时，当前这个被转换的二层接口配置信息将丢失，恢复到默认配置状态。也就是二层交换端口被转换成三层可路由端口后，原来配置的 VLAN 配置信息将丢失。

4.1.1 理解两组重要概念

在正式介绍各种交换端口的数据帧收发原理之前，先要理解两组重要概念的比较：一是 Tag（标记）和 Untag（不标记）比较；二是 PVID 与 VID 的比较。

1．Tag 与 Untag

VLAN 标记也称帧标记，是 Cisco 开发的，用于标识中继链路上的不同数据帧。它有两种不同的标记格式，那就是通用的 IEEE 802.1Q VLAN 标记和 Cisco 私用的 ISL VLAN 标记。Tag 就是在数据帧的帧头“源 MAC 地址”和“目的 MAC 地址”字段前面（ISL VLAN 标记）或后面（IEEE 802.1Q VLAN 标记）加上了一个 4B 的 VLAN 中继类型封装字段，以表明该数据帧产生于哪个 VLAN。

当一个以太网帧经过一条中继链路时，一个特定的 VLAN 标记将添加到帧中，然后再穿过中继链路。当这个数据帧到达中继链路的另一端时，原来添加的那个 VLAN 标记将被移除，然后依据交换机中的 MAC 地址列表发往正确的访问链路端口，所以数据帧在目的端口接收后并没有使用其任何 VLAN 信息，帧中的 VLAN 标记仅用作在转发数据时选择目的 VLAN 的依据（因为二层帧只能在同一个 VLAN 内转发，当然可以在三层被路由）。

Untag 就是不在帧中插入这个 VLAN 标记信息，保持数据帧原来的格式，也称本地（Native）格式。一般来说，普通 PC 机网卡只能识别不带 VLAN 标记的本地格式数据帧，不能识别带 VLAN 标记的数据帧，所以在帧到达目的主机所连接的交换端口时要去掉帧中的 VLAN 标记。有关 IEEE 802.1Q 和 ISL 这两种 VLAN 中继协议具体将在第 8 章介绍，在此不再赘述。

2．PVID 与 VID

PVID 是 Port VLAN ID（端口 VLAN ID）的简称，是指端口所属 VLAN 的 VLAN ID。VID 就是指 VLAN ID，每个 VLAN 都有一个唯一的 VLAN ID。因为访问（Access）端口仅可属于一个 VLAN，所以它的 PVID 实际上就相当于 VID（VLAN ID）。一个中继（Trunk）端口可以属于多个 VLAN，但一个 Trunk 端口只能有一个 PVID，也就是所分配给该 Trunk 端口的本地 VLAN（Native VLAN）的 VLAN ID。Trunk 端口的本地 VLAN 指定是通过 **switchport trunk native vlan** *vlan_id* 的接口配置命令进行的，也就相当于 Trunk 端口的 PVID 指定。当一个 Trunk 端口接收到一个不带 VLAN 标记的数据帧时，会打上该中继端口的 PVID 所对应的默认 VLAN ID，把这个数据帧当成该 VLAN 中的数据帧来处理；而如果接收到的是与 PVID 对应的 VLAN 中的数据帧时，则会去掉帧中的 VLAN 标记发往 PVID 对应的 VLAN 中。有关交换端口和中继端口的数据帧收发规则将在 4.1.2 节和 4.1.3 节介绍。

明白了以上两组概念后，就比较好理解下面将要介绍的各种交换端口的数据帧收发规则了。

4.1.2　Access 端口及数据帧收发规则

交换机上的绝大多数以太网接口通常都设置为 Access 端口。Access 端口通常用于直接连接终端设备，如 PC 机，也可以用于交换机间的级联，但一般不这样配置，在本节后面将有具体说明。

一个 Access 端口仅可属于并且承载一个 VLAN 内的通信（除非被配置成语音 VLAN 端口）。在 Access 端口上接收和发送的通信是不带 VLAN 标记的本地（Native）格式（因为它只能接收和发送来自或去往一个 VLAN 的数据帧），到达一个 Access 端口的通信是假定来自该 Access 端口所属的 VLAN。如果一个 Access 端口接收了一个带有标记 ISL（Inter-Switch Link，交换机间链路）或者 IEEE 802.1Q 标记的帧，则这个帧将被丢弃，Access 端口也不会学习这个数据帧的源 MAC 地址。

Access 端口的数据帧收发规则如下：

- Access 端口在收到一个数据帧（**Access 端口通常是从终端 PC 中接收数据帧**）后，先判断该数据帧中是否有 VLAN 标记信息。如果没有 VLAN 标记，则打上该 Access 端口的 PVID 后继续转发（**毕竟 Access 端口收到数据帧后是向其他端口发送的，可以识别带有 VLAN 标记的数据帧**）；如果有 VLAN 标记（**这个数据帧肯定是来自其他非 Access 端口和终端 PC，因为 Access 端口和终端 PC 网卡不会发送带 VLAN 标记的数据帧**），则默认直接丢弃。
- Access 端口上发送数据帧时，会先将数据帧中的 VLAN 信息去掉（**因为 Access 端口发送数据帧一般是到终端 PC，PC 中的网卡是不能识别 VLAN 标记的。还有一种情况是发送到另一个相同 VLAN 中的 Access 端口，因为 Access 端口也不接收带有 VLAN 标记的数据帧**），然后再直接发送，所以 Access 端口发送出去的数据帧都是不带 VLAN 标记的。

根据以上 Access 端口收发数据帧的规则可知，Access 端口可以实现同一交换机上相同 VLAN 中的主机相互通信；也可以实现交换机级联时的不同交换机中相同 VLAN 主机间的数据帧交换，但不能实现不同 VLAN 主机间的数据帧交换。如果交换机级联端口设置为 Access 端口，则两交换机只能进行级联端口所属 VLAN 主机间的通信，不能与其他 VLAN 主机间进行通信，而且两交换机的级联端口还必须添加到相同 VLAN 中。如级联的 SW1 和 SW2 交换机上都配置有 VLAN 2，并且这两个级联端口都添加到 VLAN 2 中，则 SW1 和 SW2 交换机中的 VLAN 2 中的主机间可以直接

通信。但这显然不能实现交换机级联的最终目的，所以不常用。除非级联的两个交换机的所有端口都属于同一 VLAN。

表 4-1 所示是根据上面介绍的 Access 端口接收或发送数据帧的规则而列举的示例（表中的 VLAN 2、VLAN 3 只是其中的两个 VLAN 例子，实际上可为其他任意已激活的 VLAN）。

表 4-1 Access 端口数据帧处理示例

Access 端口的 PVID	接收数据帧的 VLAN ID	发送数据帧的 VLAN ID	处理结果
VLAN 2	无	--	打上 VLAN 2 标记后继续转发
VLAN 2	VLAN 3	--	丢弃
VLAN 2	--	VLAN 2	去掉 VLAN 2 标记后继续发送
VLAN 2	--	VLAN 3	去掉 VLAN 3 标记后继续发送

Cisco 交换机支持两种类型的 Access 端口：

- 静态 Access 端口（Static Access Port）：它是被手动指派到一个 VLAN 中的（也可以通过使用 IEEE 802.1x 的 RADIUS 服务器指派）。
- 动态 Access 端口（Dynamic Access Port）：它所属的 VLAN 成员资格是通过流入的帧学习到的。默认情况下，一个动态 Access 端口是不属于任何 VLAN 的成员，仅在发现了该端口属于某个 VLAN 成员后才可以从该 VLAN 转发数据帧到该端口或者从该端口发送数据帧到该 VLAN。交换机的动态 Access 端口是通过 VMPS（VLAN Membership Policy Server，VLAN 成员策略服务器）来指派到一个 VLAN 中的。Catalyst 6500 系列交换机可以作为 VMPS，但 Catalyst 3550/3750 这样比较低端的系列交换机不能作为 VMPS 服务器。

4.1.3 Trunk 端口及数据帧收发规则

Trunk 端口通常用于交换机级联，或者交换机与路由器、防火墙的连接，用来承载多个 VLAN 的通信（**不像 Access 端口那样只能属于并承载一个 VLAN 的通信**），并且默认是 VLAN 数据帧库中的所有 VLAN 的成员。也就是说，默认情况下 Trunk 端口可以接收、转发或者发送所有来自或者到达 VTP（VLAN 中继协议）域中所有 VLAN 的数据帧，**但这并不是说 Trunk 端口可以实现不同 VLAN 间的数据帧通信，只是说它可以转发多个 VLAN 中的数据帧**。在 Cisco IOS 交换机中，有两种类型的 Trunk 端口：

- ISL Trunk 端口：ISL（Inter-Switch Link，交换机间链路）是 Cisco 设备专用的 VLAN 中继协议，用来在交换机间点对点链路上保持 VLAN 信息。**在一个 ISL 类型 Trunk 端口中，所有接收到的数据帧均将以 ISL 协议头封装，并且所有传输的数据帧都与 ISL 头一起被发送。在 ISL Trunk 端口上接收到的无 VLAN 标记帧（也称“本地帧”）都将被丢弃**。
- IEEE 802.1Q Trunk 端口：IEEE 802.1Q（英文缩写为 dot1q）是 IEEE 以标准形式发布的公用中继标准协议。IEEE 802.1Q 定义一个关于 VLAN 连接介质访问控制层（MAC）和 IEEE 802.1D 生成树协议的具体概念模型。**IEEE 802.1Q Trunk 端口同时支持加 VLAN 标记和不加 VLAN 标记的帧通信**。IEEE 802.1Q Trunk 端口分配有一个默认 PVID，把所有非标记通信都传输到默认 PVID 所对应的 VLAN 端口上，所有未标记的通信和以空 VLAN ID（也就是不存在的 VLAN ID）标记的通信都将被假设属于默认 PVID 所属的 VLAN 端口。带有与发送数据帧的端口的默认 PVID 相同的 VLAN ID 的数据帧将以不标记方式发送，带有其他 VLAN ID 的所有数据帧直接发送。

【说明】ISL 标记能与 IEEE 802.1Q 中继执行相同的 VLAN 信息中继任务，只是所采用的帧格式不同。具体的帧格式将在第 8 章介绍。

尽管默认情况下，Trunk 端口是 VTP（VLAN 中继协议）域中每个 VLAN 的成员，但仍可以通

过为每个 Trunk 端口配置允许的 VLAN 列表来限制所传输通信的 VLAN。这个 VLAN 允许列表除了关联的 Trunk 端口外，不影响其他端口。默认情况下，所有可能的 VLAN（VLAN ID 范围是 1～4094）都在允许列表中。如果 VTP 知道有这个 VLAN，并且这个 VLAN 是活动状态，则 Trunk 端口可以仅成为该 VLAN 成员；如果 VTP 学习到一个新的活动 VLAN，且该新的 VLAN 是在某个 Trunk 端口允许列表中，则 Trunk 端口自动成为这个新的 VLAN 成员，并且为该 VLAN 转发所有流经该 Trunk 端口的通信；如果 VTP 学习到了一个新的活动 VLAN，但它并不在某个 Trunk 端口的 VLAN 允许列表中，则该 Trunk 端口不会成为该 VLAN 的成员，也不会为该 VLAN 转发流经该 Trunk 端口的通信。

Trunk 端口的数据帧收发规则如下：

- 在 Trunk 端口上发送数据帧时，先会将要发送数据帧的 VLAN 标记与 Trunk 端口的 PVID 进行比较，**如果与 PVID 相等，则从数据帧中去掉 VLAN 标记再发送；如果与 PVID 不相等，则直接发送**。这样一来，如果将交换机级联端口都设置为 Trunk，并允许所有 VLAN 通过后，默认情况下除 VLAN 1 外的所有来自其他 VLAN 中的数据帧将直接发送（因为这些 VLAN 不是 Trunk 端口的默认 VLAN），而作为 Trunk 端口默认 VLAN 的 VLAN 1，则需要通过去掉数据帧中的 VLAN 信息后再发送。
- 在 Trunk 端口收到一个数据帧时，会首先判断是否有 VLAN 信息。**如果没有 VLAN 标记，则打上该 Trunk 端口的 PVID，视同该帧是来自该 Trunk 端口 PVID 所对应的 VLAN，然后把该帧转发到这个 VLAN 接口上；如果有 VLAN 标记，判断该 Trunk 端口是否允许该 VLAN 的数据帧进入，且如果该 VLAN ID 与该 Trunk 端口 PVID 相同，则去掉 VLAN 标记后转发；如果该 VLAN ID 与该 Trunk 端口 PVID 不同，则直接转发；否则丢弃**。

表 4-2 所示是根据上面介绍的 Trunk 端口接收或发送数据帧的规则而列举的示例（表中的 VLAN 2、VLAN 3 只是其中的两个 VLAN 例子，实际上可为其他任意已激活的 VLAN）。

表 4-2　Trunk 端口数据帧处理示例

Trunk 端口的 PVID	接收数据帧的 VLAN ID	发送数据帧的 VLAN ID	处理结果
VLAN 1（默认）	无	--	打上 VLAN 1 标记后转发到 VLAN 1 接口
VLAN 2	无	--	打上 VLAN 2 标记后转发到 VLAN 2 接口
VLAN 2	VLAN 2（在 Trunk 端口上允许）	--	去掉 VLAN 2 标记后转发
VLAN 2	VLAN 3（在 Trunk 端口上允许）	--	接收并转发
VLAN 2	VLAN 3（在 Trunk 端口上不允许）	--	丢弃
VLAN 2	--	VLAN 2	去掉 VLAN 2 标记后向 PVID 所对应的 VLAN 中发送
VLAN 2	--	VLAN 3	直接发送到目的 VLAN

【说明】在华为和 H3C 交换机中，除了也有 Access 和 Trunk 端口外，还有一种与 Trunk 端口类似的端口——Hybrid 端口，也与 Trunk 端口一样可以接收和发送多个 VLAN 的数据帧，但它既可以用于交换机、路由器等网络设备之间的连接，也可以用于直接连接用户计算机。Hybrid 端口和 Trunk 端口在接收数据帧时处理方法是一样的，唯一不同之处在于发送数据帧时：Hybrid 端口可以允许多个 VLAN 的数据帧发送时不打标记，而 Trunk 端口只允许与 PVID 一致的 VLAN 中的数据帧发送时不打标记，请参见与本书同时出版的《H3C 交换机配置与管理完全手册（第二版）》一书。

下面通过一个因 PVID 设置不当造成的网络故障的排除方法来加深对 Access 和 Trunk 端口数据帧收发规则的理解。在图 4-1 中，SW1 和 SW2 之间的连接链路是 Trunk 链路，允许网络中所有 VLAN 的数据帧通过。并设置 SW1 的 f0/2 Trunk 接口的 PVID=1，SW2 的 f0/1 Trunk 接口的 PVID=2，PC2～PC5 各自属于自己的 VLAN，为 Access 端口。现只有 PC2 无法上网。

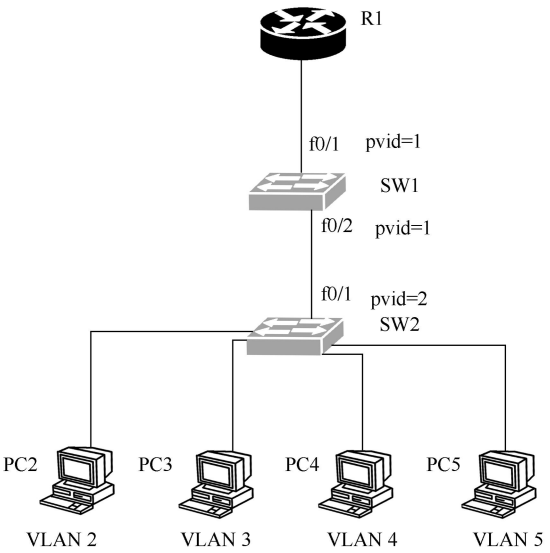

图 4-1　Access 和 Trunk 端口收发规则解析示例

这时首先分析一下 PC2 在上网时发送的数据帧流程：首先 PC2 是向所连接的 Access 端口发送不带 VLAN 标记的帧，所连的 Access 端口接收到这个帧后打上它所属的 VLAN 2 的标记转发到达 SW2 的 f0/1 Trunk 端口，经过比较发现所收到的数据帧的 VLAN 标记（2）与 SW2 的 f0/1 Trunk 端口的 PVID（2）一样，所以此时 SW2 的 f0/1 Trunk 端口会把这个数据帧去掉 VLAN 标记转发到 SW1 的 f0/2 Trunk 端口。此时因为 SW1 的 f0/2 Trunk 端口收到的数据帧没有 VLAN 标记，则直接把它打上与 SW1 的 f0/2 Trunk 端口 PVID（1）对应的 VLAN 1 标记，然后错误地把它转发到 VLAN 1 所对应的 VLAN 接口上，所以造成 PC2 不能上网。

现在再来看一下其他几台机器为什么能正常上网，以 PC3 为例。

PC3 连接的也是 SW2 上的一个 Access 端口，发送的帧也是不带标记的，所连的 Access 端口接收到这个帧后打上它所属的 VLAN 3 的标记转发到达 SW2 的 f0/1 Trunk 端口，经过比较发现所收到的数据帧的 VLAN 标记（3）与 SW2 的 f0/1 Trunk 端口的 PVID（2）不一样，所以此时 SW2 的 f0/1 Trunk 端口会直接转发这个数据帧到 SW1 的 f0/2 Trunk 端口。SW1 的 f0/2 Trunk 端口再比较自己的 PVID（1）与所收到的数据帧的 VLAN 标记（3），发现不一样，直接转发，所以 PC3 是能上网的。其他的 PC4、PC5 与 PC3 的数据帧发送流程是一样的。

从以上分析可以看出，造成 PC2 不能上网的根本原因就在于从访问端口发送的数据帧的 VLAN 标记与 SW2 的 f0/1 Trunk 端口的 PVID（2）一样，所以造成转发后的数据帧是不带 VLAN 标记的，最后被 SW1 的 f0/2 Trunk 端口错误地把这些数据帧直接转发到了它所属的 VLAN 中，而不是正确地发送到对应的 VLAN 中。这时如果把 SW2 的 f0/1 Trunk 端口的 PVID 设置成其他 PC 机在 VLAN 的 VLAN ID，则对应的 VLAN 中的 PC 机就不能上网了。所以在这种情况下，只要把 SW2 的 f0/1 Trunk 端口的 PVID 设置不包括网络中 PC 机所在 VLAN 的 VLAN ID（本示例中设置为 1）就可以确保各 VLAN 中的 PC 都可以上网。这样就可以得出这样一条经验：**要确保网络中所有 VLAN 用户都能上网，则需要把 Trunk 端口的 PVID 设置成非上网用户所在 VLAN 的 VLAN ID**。

4.1.4　Tunnel 端口

Cisco IOS 交换机中的 Tunnel 端口专用于 IEEE 802.1Q 隧道中，用来隔离一个服务提供商网络的客户与另一个使用相同 VLAN 号的客户。需要在一个服务提供商边缘交换机的 Tunnel 端口上配置一个到客户交换机的 IEEE 802.1Q Trunk 端口的非对称链路。进入客户端边缘交换机 Trunk 端口

的已经是以客户自己内部 VLAN 进行 IEEE 802.1Q 标记的数据帧，到达服务提供商边缘交换机的 Tunnel 端口后，再以服务提供商分配给客户的对应 VLAN ID 进行 IEEE 802.1Q 标记（称之为 metro 标记）封装，这样由客户发送来的帧就包括了分配每个客户的唯一的 VLAN ID。这个双重标记的数据帧通过服务提供商网络继续保持原来封装的客户内部 VLAN ID。在从服务提供商边缘交换机到另一个出口（也是 Tunnel 端口）时，metro 标记将被删除，这样就可以从客户端网络中重新得到原始 VLAN 号。

Tunnel 端口不能作为 Trunk 端口或 Access 端口，而且对于每一个客户来说，服务提供商分配给他的 VLAN ID 必须是唯一的，但客户自己内部可使用的 VLAN ID 与其他客户和服务提供商网络中的 VLAN ID 无关。这样就解决了服务提供商 VLAN ID 空间不足和同一服务提供商中不同客户使用的 VLAN ID 空间重叠的双重问题。这就是 Tunnel 端口的主要应用。

4.2　Cisco IOS 交换机的其他类型端口

除了上节介绍的 3 种二层交换端口外，在 Cisco IOS 交换机中还有一些其他端口，如可路由端口（Routed Port）、以太网通道端口组（EtherChannel Port Groups）、交换机虚拟接口（Switch Virtual Interface，SVI）和以太网管理端口（Ethernet Management Port，EMP）等，本节将集中进行介绍。

4.2.1　IOS 交换机的可路由端口

Cisco IOS 交换机上的可路由端口（Routed Port）就像路由器上的物理接口一样，属于三层端口，但它不一定非要与路由器连接，还可以与可管理的站点连接。可路由端口不会像 Access 端口那样与特定的 VLAN 关联，不会去识别经过封装成数据包后的原来帧中的 VLAN ID，因为它不需要通过二层协议进行通信，只是通过三层路由协议进行通信。每个可路由端口相当于一台独立的路由器，只认为自己所连接的是一个单独的子网。Cisco IOS 交换机上的可路由端口就像传统的路由器接口一样，可以配置三层路由协议。但运行 LAN Base 特性集的交换机不支持可路由接口和下节将要介绍的 SVI 接口。

可路由端口仅是一个三层接口，所以它不支持像 VTP、DTP（Dynamic Trunk Protocol，动态中继协议）和 STP（Spanning-Tree Protocol，生成树协议）这样的二层协议。配置可路由端口是通过 **no switchport** 接口配置命令把接口转换成三层模式，然后使用 **ip address** *ip_address* 接口配置命令为该端口分配 IP 地址，启用路由功能，并可通过 **ip routing** 和 **router** *protocol* 全局配置命令配置路由协议特性。

键入 **no switchport** 接口配置命令后将先关闭对应端口，然后再重新开启它。这时在原来连接该端口的设备端会弹出一条提示消息。在把该端口从二层模式转换成三层模式时，与之关联的配置（如添加的 VLAN 及其他二层协议配置）将丢失，恢复为三层端口的默认设置。有关可路由端口的配置将在第 6 章介绍。

尽管可路由接口与 SVI 接口有许多相似的用途（如都可以配置 IP 地址、都可以连接不同网段），但它们的工作方式还是存在区别的。如果不同交换机之间是通过 SVI 连接的，则在不同交换机间是一个二层链路。这样可以在不同交换机之间正常运行你的 STP 和其他控制通信的协议，也将把一台交换机上的 STP 域延伸到其他交换机上。如果不同交换机之间是通过可路由端口连接的，则交

换机之间有一个三层链路，并像普通的路由器端口一样工作。但在可路由端口上不能运行 STP，一台交换机上的 STP 域也不能延伸到下游的其他交换机上。可路由端口的最大不足就是每个端口都将是一个独立的网络，你将管理大量的 IP 子网，这时运行各种路由协议将是最好的选择。

4.2.2 IOS 交换机的 SVI 接口

一个交换机虚拟接口（Switch Virtual Interface，SVI）代表一个由交换端口构成的 VLAN（其实就是通常所说的 VLAN 接口），以便于实现系统中路由和桥接的功能，也就是通常所说的 VLAN 接口。一个 SVI 对应一个交换机上的一个 VLAN，不同交换机上即使是同一个 VLAN 也有不同的 SVI 接口。当需要路由 VLAN 间的流量或者桥接 VLAN 之间不可路由（如二层协议、NetBEUI、DECnet 等非路由协议）的流量的时候，都需要为相应的 VLAN 配置相应的 SVI 接口。

SVI 是虚拟接口，它既可以工作在二层也可以工作在三层。工作在二层时，它用于连接交换机上某 VLAN 中的所有端口成员，相当于这个 VLAN 中所有端口成员的二层出口；当工作在三层时，它既可作为某个 VLAN 中端口成员间的虚拟三层路由端口，实现 VLAN 内部各成员间的三层通信，又可作为这个 VLAN 中所有端口成员的统一虚拟三层出口，用于与其他 VLAN 的连接。SVI 接口是当在 **interface vlan** 全局配置命令后面键入具体的 VLAN ID 时创建的。可以用 **no interface vlan** *vlan_id* 全局配置命令来删除对应的 SVI 接口（删除 SVI 后对应的 VLAN 也就删除了），只是不能删除 VLAN 1 的 SVI 接口（VLAN 1），因为 VLAN 1 接口是默认已创建的管理 VLAN。

【说明】尽管交换机堆叠支持全部或者最多 1005 个 VLAN，这样理论上来说也就相当于可以有 1005 个 SVI，但 SVI 数和路由端口数，以及其他已配置的特征数之间的相互关系可能因硬件的局限性而影响 CPU 的性能。

SVI 是在为 VLAN 接口第一次键入 **vlan** 接口配置命令时创建的。VLAN 与 ISL 或 IEEE 802.1Q 协议中封装的中继或者 Access 端口配置的 VLAN ID 的数据帧相关联的 VLAN 标记相对应。如果需要路由 VLAN 间的通信，则需要为每个 VLAN 配置一个 SVI，并为每个 SVI 接口分配一个 IP 地址。有关 SVI 接口 IP 地址的分配方法将在第 6 章介绍。

相同或者不同交换机中同一 VLAN 中的设备可以直接进行二层通信（当然要确保在不同交换机连接的端口上允许对应 VLAN 通信地址通过），不同 VLAN 间必须通过路由器才能进行数据帧交换。在带有路由功能的交换机中，当你为不同 VLAN 配置了 SVI，并且为它们配置了 IP 地址后，则不同 VLAN 可直接通过交换机进行数据帧交换。在图 4-2 所示的示例中，通过在三层交换机上启用 IP 路由协议后，当为 VLAN 20 和 VLAN 30 的 SVI 接口配置 IP 地址时，从主机 A（Host A）可以直接通过交换机把数据帧发往主机 B（Host B），而无需另外的路由器。具体配置方法将在第 10 章介绍。

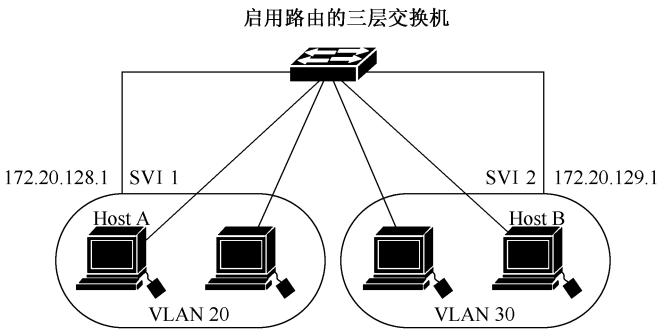

图 4-2　通过 SVI 接口进行的 VLAN 连接示意图

【说明】当在独立交换机或堆叠主交换机上运行 IP Services 特性集 IOS 映像时，交换机可以有

两种方法在接口之间通信：路由和 Fallback Bridging。而如果在独立交换机或堆叠主交换机上运行的是 IP base 特性集 IOS 映像，则仅可以通过基本的路由（包括静态路由和 RIP 协议路由）来使得交换机中不同 VLAN 间进行通信。只要可能，维持高性能是通过交换机硬件来完成的。不管如何，仅以 Ethernet II 格式封装的 IPv4 数据帧可以在硬件中被路由。非 IP 通信和带有其他封装方法的通信可以通过硬件被 Fallback Bridging。

4.2.3　IOS 交换机的 Uplink 端口

Uplink 端口就是通常所说的级联端口，专门用于与上级交换机连接，也就是通常所说的交换机级联。当然，交换机的级联不一定要使用 Uplink 端口，只是使用 Uplink 端口进行交换机级联（在交换机配备有 Uplink 端口的情况下）性能更佳。Uplink 端口与普通以太网端口最大的不同就是**它可以采用普通的直通线与上级的交换机进行连接，而不是用交叉网线连接**。

【注意】一般来说，Uplink 端口与交换机（或集线器）的第一个端口是共享通道的，所以在使用 Uplink 端口时，交换机（或集线器）的第一个普通以太网端口就不能同时用了。不过，现在的交换机通常不是共享通道的，所以还是两个端口可以同时使用，具体要看相应交换机的说明书才行。

级联扩展模式是最常见的一种端口和距离扩展方式。目前常见的交换机的级联根据交换机的端口配置情况又有两种不同的连接方式。如果交换机备有 Uplink（级联）端口，则可直接采用这个端口进行级联。不过要注意，在这种级联方式中上一层交换机所采用的仍是普通以太网端口，只是下层交换机则要采用专门的 Uplink 端口（注意，不是两端都是 Uplink 端口），如图 4-3 所示。

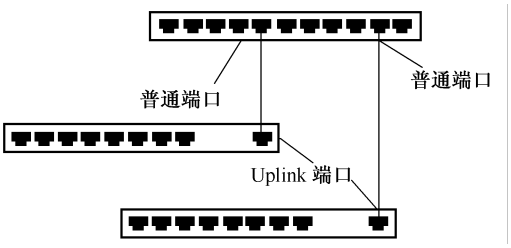

图 4-3　使用 Uplink 端口进行的交换机级联示例

这种级联方式性能比较好，因为级联端口的带宽通常是比较高的。但要注意，如果采用此种级联扩展方式，则绝大多数交换机间的级接网线必须是直通线，不能采用交叉线，而且每段网线不能超过双绞线单段网线的最大长度——100 米。当然，如果交换机端口支持 MDI/MDIX 类型自动翻转，则也可采用交叉线。

有些 Cisco 交换机（如 Catalyst 3550、Catalyst 3560 系列）还支持双用途的 Uplink 端口。每个 Uplink 端口可以看成一个带有双前端子，同时支持 RJ-45 连接器和 SFP（Small Form-factor Pluggable，小型可插式）模块连接器的单一接口，但此时也只能在同一时刻使用一种接口，即每一时刻它仅可以使用其中的一个连接器。因为这个双前端子不是接口冗余，而是多提供了一种连接器类型选择。默认情况下，交换机在第一次链路启用时动态选择接口类型。无论如何，可以使用 **media-type** 接口配置命令来手动选择 RJ-45 连接器或 SFP 模块连接器。这时，每个 Uplink 端口有两个指示灯：一个显示 RJ-45 端口状态，另一个显示 SFP 模块端口状态。灯亮时显示相应连接器是激话的。

4.2.4　IOS 交换机的 EMP

在一些 Cisco 交换机（像 Catalyst 4500、Catalyst 4900 等系列交换机）中，还可以配置以太网

管理端口（Ethernet Management Port，EMP）。在这些机型中，以太网管理端口是标注为 fa1 或 fastethernet1 的端口（也就是第一个快速以太网端口），是一个三层主机端口，用于连接 PC 机。可以使用以太网管理端口来连接到 PC 机上，替代交换机控制台（Console）端口来在浏览器中管理交换机。但首先必须为该以太网管理端口分配一个 IP 地址。以太网管理端口的连接如图 4-4 所示。

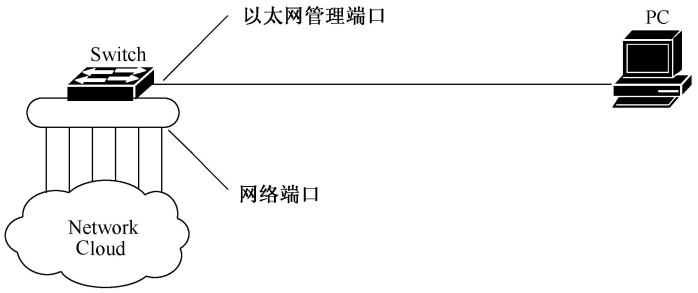

图 4-4　通过以太网管理端口连接 PC 的示意图

默认情况下，以太网管理端口是启用的。交换机不能把数据帧从以太网管理端口路由到网络端口，也不能把数据帧从网络端口路由到以太网管理端口。也就是说，以太网管理端口仅用于监控、管理。要实现这样的路由目的，fa1 接口自动置于一个分离路由域（或 VRF 域）中，称为 *mgmtVrf*。不能配置其他任何接口在同一个路由域中，也不能为 fa1 接口配置不同的路由域。EMP 是在以下型号的交换机中得到支持的：WS-C4948-10GE、ME-C4924-10GE、WS-C4948 和 WS-C4900M。

可以通过查看该端口指示灯状态来判断该端口的链路状态：指示灯为绿色，表明该端口链路处于正常活动状态；如果指示灯不亮，表明该端口链路处于关闭状态；如果指示灯为琥珀色，则表明该端口链路自检失败。配置以太网管理端口的方法与普通以太网端口的配置方法是一样的，具体将在第 6 章介绍。

4.2.5　IOS 交换机的 EPG

以太网通道端口组（EtherChannel Port Groups，EPG）把组中的多个交换端口视为一个交换端口。这些端口组在交换机之间或交换机和服务器之间担当一个具有单一高带宽连接的逻辑端口。以太网通道在一个通道中提供整个链路的通信负载平衡。如果以太网通道中的一个链路失效，流量会自动从失效链路转移到备用链路。

可以把多个 Trunk 端口组合成一个逻辑 Trunk 端口；把多个 Access 端口组合成一个逻辑 Access 端口；把多个 Tunnel 端口组合成一个逻辑 Tunnel 端口；把多个可路由端口组合成一个逻辑可路由端口。绝大多数的协议能够在单独或是组合的交换端口上运行，并且不会意识到在端口组中的物理端口，除了像 DTP（Dynamic Trunk Protocol，动态中继协议）、CDP（Cisco Discovery Protocol，思科发现协议）和 PAgP（Port Aggregation Protocol，端口聚合协议）这些只能在物理接口上运行的协议外。

当配置一个以太网通道端口组时，需要先创建一个端口通道逻辑接口，然后指派一个接口给以太网通道。对于三层接口，需要使用 **interface port-channel** 全局配置命令手动创建该逻辑接口，然后使用 **channel-group** 接口配置命令为以太网通道指派一个接口；对于二层接口，可以使用 **channel-group** 接口配置命令动态创建这个端口通道逻辑接口。这个命令就把物理接口和逻辑接口绑定在了一起。

有关以太网通道端口组的具体配置方法将在第 6 章专门介绍。

4.2.6　IOS 交换机的 PoE 端口

现在许多厂商（如 Cisco、3COM 和华为等）都推出了基于以太网供电（Power over Ethernet，PoE）的交换机技术，以解决一些电源布线比较困难的网络环境中需要部署交换机设备的问题。Cisco 推出了业界唯一支持 802.3af PoE 的 10/100/1000Mb/s 端口，这种配置在 Catalyst 6500 和 Catalyst 4500 交换机中均被支持。千兆位以太网和 PoE 相结合能够实现更出色的网络优化、用户生产效率和投资保护。此外，利用 PoE，用户无须再为每个支持 PoE 的设备提供墙壁电源，从而消除了为连接 IP 电话、无线 LAN 接入点、视频监视摄像机、建筑物管理系统和远程视频亭等设备所必须开销的电源布线成本。此外，借助 PoE，企业还能够将关键的设备锁定在一个电源上，用 UPS 备份电源支持整个系统。

Cisco Catalyst 3750 家族提供了新的支持 IEEE 802.3af 和 Cisco 预标准 PoE 的 48 端口和 24 端口快速以太网交换机。此外，Cisco 在新推出的 Catalyst 3560 家族中，48 端口和 24 端口快速以太网交换机系列支持新的业界标准和 Cisco 标准。Catalyst 3550-24 PWR 交换机将继续支持 Cisco 预标准 PoE，所有的 24 端口配置均同时支持 24 个完全供电的 PoE 端口（15.4W），实现了最出色的上电设备支持。48 端口配置以 15.4W 支持 24 个端口，以 7.7W 支持 48 个端口，或在 7.7～15.4W 之间支持 24～48 之间任意数量的端口。

Cisco Catalyst 6500 系列提供了一个新的 96 端口 10/100 线卡以及 48 端口的 10/100 和 10/100/1000 线卡。Catalyst 6500 系列为 96 端口 10/100 卡和 48 端口 10/100/1000 卡提供了一个模块化的 PoE 子卡架构，实现了最大的灵活性和投资保护。Cisco Catalyst 4500 系列也提供了新的 48 端口 10/100 和 10/100/1000 线卡。所有的线卡均支持 IEEE 802.3af 和 Cisco 预标准 PoE。这些卡兼容任何 Catalyst 6500 或 4500 机箱以及超级引擎。Catalyst 模块化机箱交换机可同时为模块上 48 个端口中的每个端口提供 15.4W。

在优势方面，PoE 技术除了从以太网电缆为连接设备提供通用供电支持外，PoE 降低了投资开支，从而降低了在统一 IP 基础设施中整合进上电设备的总部署成本。PoE 免除了为终端设备安装墙壁电源连接的需要，因而降低了与支持终端设备相关的电源插座成本。它还可以在部署本地交流电源较为困难的场所安装网络连接设备，从而提供了更大的灵活性。

Cisco 交换机 PoE 端口为以下设备连接提供电源：

- Cisco 预标准电源设备（如 Cisco IP 电话和 Cisco Aironet 访问点）
- 兼容 IEEE 802.3af 的电源设备

在 Cisco IOS 12.2(40)SE 及以前版本中，每个 10/100/1000Mb/s PoE 端口可以提供 15.4W 的电源功率到设备上。在 Cisco IOS 12.2(44)SE 及以后版本中，支持增强 PoE。增强 PoE 应该在端口上进行配置，可以为设备提供高达 20W 的电源功率，如 Cisco AP1250 的 WLAN 访问点设备。

1．支持协议和标准

Cisco 交换机使用以下协议和标准来支持 PoE：

- 带有电能的 CDP：在这种带有电能的 CDP 协议的支持下，电源设备通告交换机它可以提供的电能功率。交换机并不回应电能消息。交换机仅可以选择由 PoE 端口供电或者从 PoE 端口上移去电源。
- Cisco 智能电源管理：电源设备和交换机通过电能协商 CDP 消息（Power-negotiation CDP Messages）协商所能接受的电源功率水平。这种协商可以允许使用高电能 Cisco 电源设备，如大于 7W 的设备，工作在其最高的电能模式。
- IEEE 802.3af：这个标准最主要的功能就是电源设备发现、电源管理、连接断开检测和可

选的电源设备分类。

- IEEE 802.11n（Predraft Standard）：在这个标准的支持下，可以在一个增强型的 PoE 端口上提供高达 20W 的电能。

2．电源设备检测和初始电能分配

在 PoE 端口处于非关闭状态时，交换机可以检测到一个 Cisco 预标准或 IEEE 标准电源设备，启用 PoE 功能后（默认是启用的），连接到这个端口的设备就无须再通过交流电供电了。

交换机判断所连设备是否需要电源是依据以下几个方面的：

- Cisco 预标准电源设备在交换机检测到它时，不为它提供所需的电源，所以交换机仍会以分配 15.4W 作为电能预算的初始分配。初始电能预算就是所需的最大电源设备量。交换机在检测并接受电源设备供电时就初始化电能的分配。因为交换机需要接收从电源设备发来的 CDP 消息，而且电源设备与交换机要通过 CDP 电能协商消息进行协商，所以初始化的电能分配可能要被告知。
- 交换机会根据电能级别对检测到的 IEEE 设备进行分类。根据在电能预算中可用的电能，如果端口可以被供电，则交换机可以检测到。表 4-3 列出了这些分类级别。

表 4-3　IEEE 电源分类

IEEE 类别	交换机的最大电源需求	上电设备最大输入电量
0（默认模式）	15.4W	0.44～12.95W
1	4.0W	0.44～3.84W
2	7.0W	3.84～6.49W
3	15.4W	6.49～12.95W
4（保留）	按照类别 0 对待	按照类别 0 对待

交换机会监控和跟踪电源请求，并仅在有可用电能时许可请求。交换机跟踪电源预算（可以为交换机 PoE 端口提供的电源），在端口被许可或者被拒绝供电时重新计算电源需求，以实时更新电源预算。

管理 IP 地址就是可以用来在网络中访问（无须通过 Console 接口本地连接）交换机的 IP 地址。在这里首先要明确的一个事实是，不是只有三层交换机才有管理 IP 地址，纯二层交换机同样可以有管理 IP 地址，只要这个交换机是可网管型的就有这个管理 IP 地址。但是，三层交换机与二层交换机在管理 IP 地址的设置上还是有一些区别，那就是二层交换机只能使用特定的管理接口来配置管理 IP 地址，而三层交换机理论上可以在任意三层接口上配置管理 IP 地址。

4.3　Cisco IOS 交换机接口的基础配置与管理

交换机接口配置与管理是交换机最基础的配置和管理工作。上节介绍了在 Cisco 交换机中几种主要的二层接口类型，本节先介绍 Cisco IOS 交换机接口的基本配置方法和流程，在本章后面将要具体介绍 Cisco IOS 交换机二层以太网接口工作模式、二层接口属性的具体配置和管理方法。

4.3.1　IOS 交换机接口类型和标识

配置物理接口则要指定接口类型、堆叠成员号（仅在交换机堆叠中需要）、模块号和交换机端口号，让 IOS 系统知道你是配置哪个接口。

（1）接口类型。

在 Cisco 局域网以太网交换机中，目前主要的接口类型包括：10/100Mb/s 快速以太网（Fast

Ethernet，配置时写成 fastethernet 或 fa）接口、10/100/1000Mb/s 千兆以太网（Gigabit Ethernet，配置时写成 gigabitethernet 或 gi）接口、10000Mb/s 以太网（10-Gigabit Ethernet，配置时写成 tengigabitethernet 或 te）接口、SFP 模块千兆以太网（Small Form-factor Pluggable Module Gigabit Ethernet，配置时写成 SFP）接口。以上这些都是物理接口，还可以是交换机虚拟接口，如 VLAN 接口 SVI、以太网端口通道 EtherChannel。

（2）堆叠成员号。

堆叠成员号是标识交换机堆叠中的成员的，范围是 1～9，并且在交换机首次初始化时被分配。默认的成员号为 1。当交换机被分配了成员号后，它将一直保持该成员号，直到该交换机被分配了另一个成员号。但要注意的是，并不是所有交换机系列都支持交换机堆叠。在 Cisco 以太局域网交换机各系列中，支持堆叠的仅有 Catalyst 3750、Catalyst 3750-E、Catalyst 3560-E 三大系列。

【说明】可以在堆叠模式中使用交换机端口指示灯来识别交换机的堆叠成员号，有关交换机堆叠方面的详细信息请参见第 7 章。

（3）模块号。

模块号是交换机模块（Module）或插槽（Slot）号。对于非模块化（也就是固定配置）的交换机，默认为只有一个模块，模块号为 0。当然非模块交换机在配置时也不用把模块号写出来。

（4）端口号。

端口号是交换机上的接口号。接口号总是从 1 开始，排列顺序总是从面对交换机前面板时的最左边开始。

如果是堆叠交换机，交换机接口的标识顺序为：接口类型 堆叠成员号/模块号/接口号。可堆叠的独立交换机的成员号为1，非模块交换机的模块号默认为0。如一个非模块交换机的第一个堆叠成员的第一个接口为快速以太网接口，则该接口的标识为：fastethernet1/0/1（或 fa1/0/1），也可以直接写成 fa1/1，而省略模块号不输入。如果一个非模块交换机的第一个堆叠成员的第一个接口为千兆以太网接口，则它的标识为：gigabitethernet1/0/1（或 gi1/0/1），同样也可以写成 gi1/1，而不输入模块号。

对于独立模块交换机则接口标识顺序为：接口类型 模块号/接口号，如 fastethernet0/1（或 fa0/1）；而对于独立非模块交换机，可直接以接口类型+接口号来标识，如 fa1 代表 1 号快速以太网接口。

尽管在本书中，关于接口标识方面的参数名称可能不一样，如有的表示为 *type interface_id*，有的表示为 *type mod/port*，还有的是 *type slot/port – port* 等，其实最终的总体表示形式都是一样的，那就是“接口类型 接口所在模块号/接口号”。当然对于是否是模块结构，是否支持堆叠，具体的表示形式还要参见本节前面的介绍。不要被这不同的参数名搞晕了头。

另外，在网络设备中，除了物理接口这一说法外，还有一种称为“子接口”（Subinterface）的说法。它是物理接口中的虚拟接口。子接口的表示形式是在物理接口后面加上一个小圆点，然后再加上一个子接口号，如 f0/1.1，则表示 0 模块第 1 个接口的第 1 个子接口。要注意的是，它是虚拟接口，不是物理接口。

进入接口配置模式的命令为 **interface**。可以使用 **show interfaces** 特权模式命令显示特定接口或所有接口信息。下面是一些在具体配置中标识接口的示例。

以下是一个在可堆叠的独立交换机上进入端口 4 的 10/100/1000Mb/s 接口配置模式的示例。

```
Switch(config)#interface gi1/0/4
```

以下是一个在交换机堆叠成员 3 上进入端口 4 的 10/100Mb/s 接口配置模式的示例。

```
Switch(config)#interface fa3/0/4
```

以下是一个在可堆叠的独立交换机上进入端口 1 的 10-Gigabit 模块接口配置模式的示例。

```
Switch(config)#interface te1/0/1
```

以下是一个在交换机堆叠成员 3 上进入端口 1 的 10-Gigabit 模块接口配置模式的示例。

```
Switch(config)#interface te3/0/1
```

以下是一个在非可堆叠的交换机上进入端口 2 的 10/100/1000Mb/s 接口配置模式的示例。

```
Switch(config)#interface gi0/2
```

如果交换机有 SFP 模块，这些端口的接口号要依据交换机上其他接口的类型而定。如果其他接口为快速以太网类型，则 SFP 模块中的端口号从 1 开始编号；如果交换机中的其他端口也是千兆以太网类型，则 SFP 模块的接口与其他接口一起连续编号。

以下是一个在一个有 24 口 10/100/1000Mb/s 端口的可堆叠交换机上进入 SFP 模块接口配置模式的示例（SFP 模块端口编号是 25，因为前面 24 个端口都是千兆以太网端口，所以采取连续编号规则）。

```
Switch(config)#interface gi1/0/25
```

如果以上是非可堆叠交换机，则以上配置命令如下（接口标识前没有堆叠成员号 1）：

```
Switch(config)#interface gi0/25
```

以下是一个在一个有 24 口 10/100Mb/s 端口的可堆叠交换机上进入 SFP 模块接口配置模式的示例（SFP 模块端口编号是 1，因为前面 24 个端口都是快速以太网端口，所以 SFP 端口重新从 1 开始编号）。

```
Switch(config)#interface gi1/0/1
```

如果以上是非可堆叠交换机，则以上配置命令如下（接口标识前没有堆叠成员号 1）：

```
Switch(config)#interface gi0/1
```

4.3.2 IOS 交换机物理以太网接口配置流程

下面是配置 Cisco IOS 系统交换机物理以太网接口的通用配置流程，像 SVI、以太网通道这类虚拟接口的配置将在第 6 章具体介绍。

（1）在特权模式提示下键入 **configure terminal**（可以简写成 con t）命令，进入全局配置模式。按 Enter 键则显示如下提示（要注意，此时提示符已发生了改变，从特权模式提示符#改变为全局配置模式提示符(config)#）：

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

（2）在全局配置模式下按照如下格式输入：**interface** *以太网接口类型 堆叠成员号*（非可堆叠交换机不用此标识）/*模块号*/*接口号*。在此以堆叠成员 1 的千兆以太网端口 1 为例（交换机为非模块交换机，模块号默认为 0）。

```
Switch(config)#interface gi1/0/1
Switch(config-if)#
```

【注意】在接口类型和接口号之间可以留空格，也可以不留空格。当然可以是接口类型全称，也可以是简写。如 gigabitethernet 1/0/1、gigabitethernet1/0/1、gi 1/0/1 或 gi1/0/1 都是正确的。

下面是一个综合以上两步进入交换机的 Fast Ethernet interface 5/5 接口配置模式的示例。

```
Switch#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)#interface fastethernet 5/5
Switch(config-if)#
```

（3）可以使用各种接口配置命令来配置相应接口属性，具体将在本章后面和第 6 章分别介绍二层/三层接口属性配置时体现。配置完后可用 **end** 命令或者按 **Ctrl+Z** 组合键返回到特权模式。

为了提高配置效率，也可以使用 **interface range** 或 **interface range macro** 全局配置命令来配置

接口范围。但在接口范围中的接口类型必须一致，而且必须以相同的特性选项进行配置。具体在下面两小节中介绍。

4.3.3　IOS 交换机以太网接口范围配置

因为在一个交换机上同类型、同用途的以太网接口往往不止一个，所以它们经常是属性配置完全一样。为了提高配置效率，通常是想一次性配置这些需要相同配置的以太网接口。这时就可以使用 **interface range** 全局配置模式命令来用相同的配置参数一次性配置多个接口了。在进入接口范围配置模式时，键入的所有参数将同样应用到范围中的所有接口。这个问题其实在与网友的交流中有许多人经常会问到，这证明 Cisco 早已考虑到我们的诉求（H3C 交换机中也有类似的功能）。具体的接口范围配置步骤如表 4-4 所示（从特权模式开始）。

表 4-4　接口范围配置步骤

步骤	命令	用途说明
1	Switch#**configure terminal**	进入全局配置模式
2	Catalyst 2950/2960/3750 等非模块交换机系列： Switch(config)#**interface range** {*port-range* | **macro** *macro_name*} Catalyst 4000/4500/4900 等模块交换机系列： Switch(config)#**interface range** {**vlan** *vlan_ID - vlan_ID*} | {{**fastethernet** | **gigabitethernet** | **tengigabitethernet** | **macro** *macro_name*} *slot/interface - interface*} [**,** {**vlan** *vlan_ID - vlan_ID*} {{**fastethernet** | **gigabitethernet** | **tengigabitethernet** | **macro** *macro_name*} *slot/interface - interface*}] Catalyst 6000/6500 系列： Switch(config)#**interface range** {{**vlan** *vlan_ID - vlan_ID* [**, vlan** *vlan_ID - vlan_ID*]} | {*type slot/port - port* [**,** *type slot/port - port*]} | {*macro_name* [**,** *macro_name*]}}	不同系列，该命令的语法格式有所不同，但总体格式是一样的，也就是一个接口范围或者再加一个定义的宏名。只不过，表示的方式有所不同。 后面两个格式中的 *vlan_ID - vlan_ID* 也属于最前面的那个格式中参数 *port-range* 的一种格式。而且后面两个格式其实是一样的，只是在接口范围表示形式和参数顺序排列上有少许不同。 参数 *port-range* 用来指定要配置的接口范围（VLAN 或者物理端口），进入接口范围配置模式。 可以使用 interface range 命令配置多达 5 个端口的范围或者以前定义的宏（macro）。有关宏方面的说明，将在下节的“配置和使用接口范围宏”中介绍。 在以英文逗号（,）分隔的接口范围中，必须为每个接口条目键入接口类型，在逗号的前后都必须有空格。 在连接符（-）格式的接口范围中，不需要重复键入接口类型，但在连接符前留有一个空格
3	使用普通配置命令来为范围中的所有接口应用配置参数	
4	Switch(config-if)#**end**	返回到特权模式
5	Switch#**show interfaces** [*interface-id*]	校验范围中的接口配置
6	Switch#**copy running-config startup-config**	（可选）保存配置更改到配置文件中

在使用 **interface range** 全局配置命令时，注意以下事项：

- 以下接口范围格式才是有效的：
  - **vlan** *vlan-ID - vlan-ID*（VLAN ID 的范围是 1～4094）
  - **fastethernet** *stack member/module/*{*第一个端口*} - {*最后一个端口*}（模块号全为 0）
  - **gigabitethernet** *stack member/module/*{*第一个端口*} - {*最后一个端口*}（模块号全为 0）
  - **port-channel** *端口通道号 – 端口通道号*（端口通道号的范围为 1～48，但必须都是激活的）
- 连接符两端必须留有空格，如 **interface range gigabitethernet1/0/1 - 4** 是有效的，而 **interface range gigabitethernet1/0/1-4** 是无效的。
- **interface range** 命令仅适用于已用 **interface vlan** 配置的 VLAN 接口（此处只是针对 VLAN 接口而言，并非指 **interface range** 命令中只能包括 VLAN 接口）。范围中的 VLAN 接口必须已用 **interface vlan** 命令进行了配置。可以用 **show running-config** 特权模式命令显示 VLAN 接口配置，不在该命令输出中显示的 VLAN 接口不能在接口范围中。
- 在范围中定义的所有接口必须是同种类型的（如全部为快速以太网、千兆以太网、以太网通道、VLAN 端口类型）。

下面的示例显示了在 Catalyst 3750 系列交换机中如何使用 **interface range** 全局配置模式命令设置堆叠成员 1 的 1～4 号快速以太网端口。

```
Switch#configure terminal
Switch(config)#interface range gigabitethernet1/0/1 – 4
Switch(config-if-range)#speed 100
```

【示例 1】在 Catalyst 3750 交换机堆叠中使用逗号分隔的堆叠成员 1 的 1～3 号快速以太网端口和堆叠成员 2 的 1～2 号千兆以太网端口上应用帧的流控制。

```
Switch#configure terminal
Switch(config)#interface range fastethernet1/0/1 - 3, gigabitethernet2/0/1 - 2
Switch(config-if-range)#flowcontrol receive on
```

如果在接口范围配置模式中键入了多个配置命令，则每个命令在键入后即被执行，而不会批量执行，也不会等到退出接口范围配置模式才执行。如果在执行过程中退出了接口范围配置模式，则有些命令可能不会在范围中的所有接口上执行。所以，必须在出现命令提示符后才退出接口范围配置模式。

【示例 2】在 Catalyst 4500/4900/6000/6500 等系列交换机中一次性激活接口 5/1～5/5。

```
Switch(config)#interface range fastethernet 5/1 - 5
Switch(config-if)#no shutdown     # 激活接口
Switch(config-if)#
*Oct    6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1, changed state to up
*Oct    6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/2, changed state to up
*Oct    6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/3, changed state to up
*Oct    6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/4, changed state to up
*Oct    6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/5, changed state to up
*Oct    6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
5, changed state to up
*Oct    6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
3, changed state to up
*Oct    6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
4, changed state to up
Switch(config-if)#
```

【示例 3】在 Catalyst 4500/4900/6000/6500 等系列交换机中在使用逗号分隔的不同类型接口范围内激活端口 5/1～5/5 快速以太网端口和 1/1、1/2 千兆以太网端口。

```
Switch(config-if)#interface range fastethernet 5/1 - 5, gigabitethernet 1/1 - 2
Switch(config-if)#no shutdown
Switch(config-if)#
*Oct    6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/1, changed state to up
*Oct    6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/2, changed state to up
*Oct    6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/3, changed state to up
*Oct    6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/4, changed state to up
*Oct    6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/5, changed state to up
*Oct    6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet1/1, changed state to
 up
*Oct    6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet1/2, changed state to
 up
*Oct    6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
5, changed state to up
*Oct    6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
3, changed state to up
*Oct    6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/
4, changed state to up
Switch(config-if)#
```

4.3.4 IOS 交换机以太网接口范围宏配置

可以创建一个接口范围宏来自动选择一个用于配置的接口范围，但是在 **interface range macro** 全局配置命令字符中使用 **macro** 关键字之前必须使用 **define interface-range** 全局配置命令来定义所要使用的宏。

定义宏的具体步骤如表 4-5 所示（从特权模式开始）。

表 4-5　定义宏的步骤

步骤	命令	用途说明
1	Switch#**configure terminal**	进入全局配置模式
2	Catalyst 2950/2960/3650/3750 等非模块交换机系列： Switch(config)#**define interface-range** *macro_name interface-range* Catalyst 4000/4500/4900 模块交换机系列： Switch(config)#**define interface-range** *macro_name* {**vlan** *vlan_ID - vlan_ID*}	{{**fastethernet**	**gigabitethernet**} *slot/interface - interface*} [**,** {**vlan** *vlan_ID - vlan_ID*} {{**fastethernet**	**gigabitethernet**} *slot/interface - interface*}] Catalyst 6000/6500 系列： Switch(config)#**define interface-range** *macro_name* {**vlan** *vlan_ID - vlan_ID*}	{*type slot/port - port*} [**,** {*type slot/port - port*}]	定义接口范围宏，并保存在交换机的 NVRAM 中。 参数 *macro_name* 是一个最大 32 个字符的宏名称字符串，一个宏最多可以包括 5 个以逗号分隔的接口范围。 每个接口范围中必须包括相同类型的端口。 这 3 种语法格式总体来说也是一样的，只是接口范围表示形式不同而已 可以使用 **no define interface-range** *macro_name* 全局配置命令删除宏
3	Switch(config-if)#**interface range macro** *macro_name*	从保存的 *macro_name* 参数宏指定的值中选择用于配置的接口范围
4	使用普通配置命令来对宏中所定义的所有接口应用配置	
5	Switch(config-if)#**end**	返回到特权模式
6	Switch#**show running-config	include define**	显示宏配置中定义的接口范围
7	Switch#**copy running-config startup-config**	（可选）保存以上设置更改到配置文件中

在使用 **define interface-range** 全局配置命令时，需要注意以下事项：

- 有效的接口范围格式如下：
  - **vlan** *vlan-ID - vlan-ID*（VLAN ID 的范围是 1～4094，有关 VLAN 接口的配置将在第 8 章介绍）
  - **fastethernet** *stack member/module/{第一个端口} - {最后一个端口}*（模块号全为 0）
  - **gigabitethernet** *stack member/module/{第一个端口} - {最后一个端口}*（模块号全为 0）
  - **port-channel** *端口通道号 – 端口通道号*（端口通道号的范围为 1～48，但必须都是激活的）
- 在键入接口范围时，必须在连接符两端留有一个空格。如 gigabitethernet1/0/1 - 4 格式是有效的，而 gigabitethernet1/0/1-4 格式无效。
- 范围中的 VLAN 接口必须已用 **interface vlan** 命令进行了配置，此时可以用 **show running-config** 特权模式命令显示 VLAN 接口配置，不在该命令输出中显示的 VLAN 接口不能在接口范围中。
- 在一个范围中定义的所有接口必须是相同的类型，但是在一个宏中可以组合多个接口类型，不同接口类型的范围用英文逗号（,）分隔。

以下示例显示了如何定义一个名为 *enet_list* 的接口范围，范围中包括了堆叠成员 1 的 1～2 号端口，并校验宏配置。

```
Switch#configure terminal
Switch(config)#define interface-range enet_list gigabitethernet1/0/1 - 2
Switch(config)#end
Switch#show running-config | include define
Define interface-range enet_list GigabitEthernet1/0/1 – 2
Switch#
```

以下示例显示了如何创建一个名称为 1 的多接口宏。

```
Switch#configure terminal
Switch(config)#define interface-range macro1 fastethernet1/0/1 - 2, gigabitethernet1/0/1 - 2
Switch(config)#end
```

以下示例显示了如何进入接口范围 *enet_list* 宏的接口范围配置模式。

```
Switch#configure terminal
Switch(config)#interface range macro enet_list
Switch(config-if-range)#
```

以下示例显示了如何删除接口范围 *enet_list* 宏，并校验是否真正删除了。

```
Switch#configure terminal
Switch(config)#no define interface-range enet_list
Switch(config)#end
Switch#show run | include define
Switch#
```

4.3.5 IOS 交换机接口配置信息查看

在配置好一个接口后，可以在特权模式下使用一系列与交换机接口相关的 **show interfaces** 特权模式命令查看、校验对应或者所有接口配置信息是否正确和数据帧通信统计信息。这个 **show interfaces** 命令功能非常强大，可选项和参数也非常多，可以选择性地查看任何与接口相关的信息，非常方便、实用。在实际的交换机维护与管理工作中经常要用到。

在 Cisco Catalyst 2900/2950/2960 等早期系列交换机中完整的命令格式如下：

show interfaces [*interface-id* | **vlan** *vlan-id*] [**accounting** | **capabilities** [**module** *number*] | **counters** | **description** | **etherchannel** | **flowcontrol** | **pruning** | **stats** | **status** [**err-disabled**] | **switchport** [**backup** | **module** *number*] | **transceiver** | **properties** | **detail** [**module** *number*] | **trunk**] [| {**begin** | **exclude** | **include**} *expression*]

在 Cisco Catalyst 3650/3750 系列可堆叠交换机中完整的命令格式如下（与上面 Cisco Catalyst 2900/2950/2960 等早期系列交换机中的该命令格式相比只是少部分选项有差异）：

show interfaces [*interface-id* | **vlan** *vlan-id*] [**accounting** | **capabilities** [**module** *number*] | **counters** | **description** | **etherchannel** | **flowcontrol** | **private-vlan mapping** | **pruning** | **stats** | **status** [**err-disabled**] | **switchport** [**backup** | **module** *number*] | **tengigabitethernet** *interface-id* | **transceiver** [**detail** | **properties** | **dom-supported-list**] [**module** *number*] | **trunk**] [| {**begin** | **exclude** | **include**} *expression*]

在 Cisco Catalyst 4500/4900/6500 等非可堆叠模块交换机系列中，完整的命令格式如下（注意，虽然这些交换机集成在 **show interfaces** 命令的可选项较少，但其实其他选项均有对应的 **show interfaces** 命令）：

show interfaces [{{**fastethernet** *mod/interface-number*} | {**gigabitethernet** *mod/interface-number*} | {**tengigabitethernet** *mod/interface-number*} | {**null** *interface-number*} | **vlan** *vlan_id*} | **status**}]

以上 **show interfaces** 命令中的可选项和参数说明如表 4-6 所示。

表 4-6 **show interfaces** 命令的可选项和参数说明

可选项和参数	说明
interface-id	（可选）指定要显示信息的物理接口（包括接口类型和接口号标识，包括接口类型、堆叠成员号（仅适用于堆叠交换机）、模块的端口号）或者端口通道，端口通道的范围为 1～48
vlan *vlan-id*	（可选）要显示的 VLAN 接口的 ID，取值范围为 1～4094
accounting	（可选）显示指定接口或端口通道的统计信息，包括活动协议和接收/发送的数据帧流量，但仅显示软件进程中的帧信息，不显示硬交换中的帧信息
capabilities	（可选）显示所有接口或者指定接口性能（也就是属性配置），包括接口功能以及你可以在对应接口上配置的选项。此选项不适用于 VLAN 接口
module *number*	（可选）显示交换机或者指定堆叠成员号的成员交换机上的所有接口的性能、交换端口配置或者数据帧收发特性。 【说明】在 Catalyst 3750 系列交换机中，参数 *number* 的取值范围为 1～9；在 Catalyst 3560 系列交换机中，参数 *number* 的取值仅可以为 1。如果你键入了指定的接口 ID，则这个选项无效
counters	（可选）显示指定接口的各种信息统计器内容，与 **show interfaces counters** 命令功能类似
description	（可选）显示指定接口或者端口通道的管理状态和描述设置
etherchannel	（可选）显示接口的以太网通道信息，可查看对应接口是否属于某个以太网通道
flowcontrol	（可选）显示接口流量控制信息，以查看接口是否配置了流量控制设置
pruning	（可选）显示接口中继 VTP 修剪信息
private-vlan mapping	（可选）显示 SVI 接口的 PVLAN（私有 VLAN）映射信息，但不适用于运行 LAN Base 特性集 IOS 系统的交换机
stats	（可选）显示接口在交换路径中接收/发送的数据帧数
status	（可选）显示接口状态，如果在状态信息中的 type（类型）字段中显示为 *unsupported*，则表示在模块中插入了不是 Cisco 支持的 SFP 模块

续表

可选项和参数	说明
err-disabled	（可选）显示出错处于禁止状态的接口
switchport	（可选）显示交换端口（不包括可路由端口）的管理和运行状态，如端口阻塞和被保护设置
backup	（可选）显示指定接口的链路备份接口配置和状态
tengigabitethernet	显示 10Gb/s 模块中的接口状态
transceiver [**detail** | **properties** | **dom-supported-list**]	（可选）显示 SFP 模块接口物理属性，与 **show interfaces transceivers** 命令功能相似
trunk	显示接口中继信息，如果你不指定任何接口，则仅显示当前活动的中继接口信息
| begin	（多选一选项）显示自第一个包括参数 expression 表达式开始以后行的输出信息
| exclude	（多选一选项）显示不包括参数 expression 表达式的行的输出信息
| include	（多选一选项）显示包括参数 expression 表达式的行的输出信息
expression	（可选项）设置一个用于限制显示输出信息的表达式，注意表达式是区分大小写的

要清除在 **show interfaces** 命令中显示的接口计数器，可以使用 **clear counters** [*interface-id*]特权模式命令进行。

【示例 1】清除和重置 fa5/5 接口上的计数器。

```
Switch#clear counters fa5/5
Clear "show interface" counters on this interface [confirm] y
Switch#
*Sep 30 08:42:55: %CLEAR-5-COUNTERS: Clear counter on interface FastEthernet5/5
by vty1 (171.69.115.10)
Switch#
```

【注意】如果使用没有带任何参数的 **clear counters** 特权模式命令，则会从所有接口中清除所有接口的计数器。**clear counters** 命令不清除用于检索 SNMP 的计数器，仅能清除显示在 **show interfaces** 命令输出中的计数器。

可以用 **shutdown** 接口配置模式命令来禁用一个接口，此时会禁用指定接口的所有功能，并在所有监控命令输出显示中标记该接口为不可用状态。这个信息会通过所有动态路由协议传达到其他网络服务器中。这样任何路由更新都不会与该接口关联了。

【示例 2】关闭交换机上的 fastethernet 5/5 接口。

```
Switch(config)#interface fastethernet 5/5
Switch(config-if)#shutdown
Switch(config-if)#
*Sep 30 08:33:47: %LINK-5-CHANGED: Interface FastEthernet5/5, changed state to a
administratively down
Switch(config-if)#
```

【示例 3】重启上面示例的 fastethernet 5/5 接口。

```
Switch(config-if)#no shutdown
Switch(config-if)#
*Sep 30 08:36:00: %LINK-3-UPDOWN: Interface FastEthernet5/5, changed state to up
Switch(config-if)#
```

要验证接口是否被禁用了，可以键入 **show interfaces** 特权模式命令来查看。禁用了的接口将显示 administratively down。

【示例 4】使用不带可选项的 **show interfaces** 命令查看堆叠成员 3 交换机上的 gigabitethernet3/0/2 接口信息。

```
Switch#show interfaces gigabitethernet3/0/2
GigabitEthernet3/0/2 is down, line protocol is down     !--显示这个接口当前是关闭的，当前链路没有启用。从中可以看出该接口是否
                                                        !--工作正常
  Hardware is Gigabit Ethernet, address is 0009.43a7.d085 (bia 0009.43a7.d085)   !--显示该接口的 MAC 地址
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
  !--以上两行显示的是接口的 MTU（最大传输单元）、BW（带宽）、DLY（链路延时）、reliability（可靠性，255/255 表示 100%可
  !--靠）、txload（发送负载，1/255 表示发送负载很小，只占了 1/255）、rxload（接收负载，与 txload 一样计算）
  Encapsulation ARPA, loopback not set     !--显示这个以太网接口的链路封装协议为 APPA，没设置 lookback 接口
```

```
Keepalive set (10 sec)     !--表示在没有负载的情况下，该接口保持激活的时长为 10 秒
Auto-duplex, Auto-speed     !--显示该接口是自动双工模式和速率配置
input flow-control is off, output flow-control is off     !--显示该接口上没有设置接收/发送流量控制
ARP type: ARPA, ARP Timeout 04:00:00 Last input never, output never, output hang never
Last clearing of "show interface" counters never     !--显示从没有进行统计器清理
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0     !--显示该接口上接收的数据帧大小/最大值/丢弃数据帧量/泛洪
                                                                          !--数据帧量和从该接口上丢弃的发送数据帧总和
Queueing strategy: fifo
Output queue :0/40 (size/max)     !--显示发送的数据帧大小/最大值
5 minute input rate 0 bits/sec, 0 packets/sec     !--显示最近 5 分钟接收数据帧速率和帧传输率
5 minute output rate 0 bits/sec, 0 packets/sec       !--显示最近 5 分钟发送数据帧速率和帧传输率
  2 packets input, 1040 bytes, 0 no buffer       !--显示该接口上已接收的帧数和数据帧大小，有多少个帧在缓存中
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles     !--显示接收到的广播和组播帧数、小于 64KB 的帧数、超过 MTU 值的帧数、
                                                            !--接收缓存时间计数器清零次数（广播风暴可能引起这个计时器清零）
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored      !--显示接收数据帧传输时出现的错误次数、CRC 失配次数、接收到的含有
                                                            !--不正确 CRC 值和整数个八位组帧数、溢出的数据帧数、忽略的数据帧数
  0 input packets with dribble condition detected     !--检测到的数据帧接收碰撞次数
  4 packets output, 1040 bytes, 0 underruns     !--显示发送的数据帧数、发送数据帧大小、欠载（也就是非线速）发送的数据帧数
  0 output errors, 0 collisions, 3 interface resets     !--显示数据帧发送错误数、碰撞数、接口重置次数
  0 babbles, 0 late collision, 0 deferred     !--显示发生串扰的次数、最近碰撞的次数、发生延时的次数
  0 lost carrier, 0 no carrier, 0 PAUSE output     !--显示丢失的载波检测数、非载波个数、脉冲流出数
  0 output buffer failures, 0 output buffers swapped out     !--显示流出缓存失效次数、流出缓存交换超时次数
```

【示例 5】使用 **show interfaces accounting** 命令查看交换机上所有接口的统计信息（也可只显示指定接口的统计信息）。输出信息中的 Protocol 是指对应接口相应通信的通信协议，Pkts In 是指对应接口接收到的相应协议通信数据帧，Chars In 指对应接口接收到的相应协议通信数据帧中所含的字符数，Pkts In 是指对应接口发送的相应协议通信数据帧，Chars In 指对应接口发送的相应协议通信数据帧中所含的字符数。

从这些统计信息中就可以分析出某个接口的工作状态是否正常，如是否只有流入的而没有流出的数据帧，或者相反，这时就要检查连接对应接口的电缆或者接口本身了。

```
Switch#show interfaces accounting
Vlan1
                Protocol        Pkts In   Chars In   Pkts Out   Chars Out
                IP              1094395   131900022  559555     84077157
                Spanning Tree   283896    17033760   42         2520
                ARP             63738     3825680    231        13860
Interface Vlan2 is disabled
Vlan7
                  Protocol      Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
Vlan31
                  Protocol      Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.

GigabitEthernet1/0/1
                  Protocol      Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.
GigabitEthernet1/0/2
                  Protocol      Pkts In   Chars In   Pkts Out   Chars Out
No traffic sent or received on this interface.

<省略>
```

【示例 6】使用 **show interfaces capabilities** 命令查看交换机上 gigabitethernet1/0/2 接口的性能。包括交换型号（Model）、接口类型（Type）、速率（Speed）、双工模式（Duplex）、中继封装协议类型（Trunk encap. type）、中继模式（Trunk mode）、广播帧抵制比率（Broadcast suppression）、流量控制（Flowcontrol）、QoS 计划（QoS scheduling）和交换机端口分析仪（SPAN）设置，以及是否属于以太网通道（Channel）、是否支持快速启动（Fast start）、是否支持服务分类重写（CoS

rewrite）、是否支持服务类型重写（ToS rewrite）、是否支持单向链路检测（UDLD）、是否有内置电源（Inline power）、是否启用端口安全保护（PortSecure）、是否启用了 IEEE 802.1x 安全认证（Dot1x）。在出现某些故障时就可以从中检查对应接口的配置是否正确，这也是日常交换机维护和管理中经常要做的一项工作。

```
Switch#show interfaces gigabitethernet1/0/2 capabilities
GigabitEthernet1/0/2
  Model:                    WS-xxxxxxxx
  Type:                     10/100/1000BaseTX
  Speed:                    10,100,1000,auto
  Duplex:                   full,auto
  Trunk encap. type:        802.1Q,ISL
  Trunk mode:               on,off,desirable,nonegotiate
  Channel:                  yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:              rx-(off,on,desired),tx-(none)
  Fast start:               yes
  QoS scheduling:           rx-(not configurable on per port basis),tx-(4q2t)
  CoS rewrite:              yes
  ToS rewrite:              yes
  UDLD:                     yes
  Inline power:             no
  SPAN:                     source/destination
  PortSecure:               yes
  Dot1x:                    yes
```

【示例 7】使用 **show interfaces description** 命令查看交换机上 gigabitethernet1/0/2 接口的描述。

```
Switch#show interfaces gigabitethernet1/0/2 description
Interface Status         Protocol Description
Gi1/0/2     up           down     Connects to Marketing
```

【示例 8】使用 **show interfaces etherchannel** 命令查看交换机上的以太网通道配置信息。从中可以看出这台交换机上配置了 3 个以太网通道，并且从中可以看出每个以太网通道的端口成员和使用状态。在我们配置以太网通道或者在使用以太网通道出现故障时就可以通过这个命令来检查，看看某个接口是否仍在某个以太网通道中。

```
Switch#show interfaces etherchannel
----
Port-channel1:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/1          Number of ports = 0
GC                  = 0x00000000    HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse

Port-channel2:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/2          Number of ports = 0
GC                  = 0x00000000    HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse

Port-channel3:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/3          Number of ports = 0
GC                  = 0x00000000    HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse
```

【示例 9】使用 **show interfaces private-vlan mapping** 命令查看交换机上的 PVLAN 映射信息。输出信息中显示交换机上的 PVLAN 是把 VLAN 10 作为主 VLAN，而 VLAN 501 和 VLAN 502 作为从 VLAN 配置的。有关 PVLAN 方面的配置请参见第 9 章。

```
Switch#show interfaces private-vlan mapping
Interface Secondary VLAN Type
```

```
--------- --------------- -----------------
vlan10      501             isolated
vlan10      502             community
```

【示例 10】使用 **show interfaces pruning** 命令查看交换机 gigibitethernet1/0/2 接口的 VTP 修剪设置。从输出信息中可以看出，gigibitethernet1/0/2 接口已启用了 VLAN 3 和 VLAN 4 这两个 VLAN，可以在这个接口上中继，VLAN 1、VLAN 2 和 VLAN 3 有向 gigibitethernet1/0/2 接口发出通信请求。有关 VTP 修剪将在第 8 章中具体介绍。

```
Switch#show interfaces gigibitethernet1/0/2 pruning
Port      Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

Port      Vlans traffic requested of neighbor
Gi1/0/2   1-3
```

【示例 11】使用 **show interfaces stats** 命令查看交换机上的 VLAN 1 接口在交换路径中接收/发送的数据帧数。输出信息中的几个字段与示例 2 中 **show interfaces accounting** 命令输出信息中的字段基本一样，只是前面的 Switching path 字段不一样，它是指出相应通信的交换路径。同样可通过此命令查看某个接口的接收/发送数据帧状态是否正常。

```
Switch#show interfaces vlan 1 stats
Switching path      Pkts In   Chars In    Pkts Out   Chars Out
          Processor   1165354  136205310     570800    91731594
       Route cache         0          0          0           0
             Total   1165354  136205310     570800    91731594
```

【示例 12】使用 **show interfaces status** 命令查看交换机上的所有接口状态，其中包括每个接口的当前连接状态、所属 VLAN、双工模式、速率和接口类型。通过此命令可以检查交换机上所有接口的当前工作状态是否正常和这些接口的基本属性设置是否正确。

```
Switch#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/1                      connected    routed     a-half  a-100 10/100/1000BaseTX
Gi1/0/2                      notconnect   121,40       auto   auto 10/100/1000BaseTX
Gi1/0/3                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi1/0/4                      notconnect   18           auto   auto Not Present
Gi1/0/5                      connected    121        a-full a-1000 10/100/1000BaseTX
Gi1/0/6                      connected    122,11     a-full a-1000 10/100/1000BaseTX

<output truncated>
Gi2/0/1                      notconnect   1            auto   auto 10/100/1000BaseTX
Gi2/0/2                      notconnect   1            auto   auto unsupported

<省略>
```

【示例 13】使用 **show interfaces** gigabitethernet1/0/20 **status** 命令查看交换机上 gigabitethernet1/0/20 接口的状态。这个命令与上面的示例用途差不多，只是这里是用来查看个别接口的工作状态和属性设置。

```
Switch#show interfaces gigabitethernet1/0/20 status
Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/20                     connected    20         a-full  a-100 10/100BaseTX
```

【示例 14】使用 **show interfaces status err-disabled** 命令查看交换机上因发生错误而被禁止的接口状态和发生错误的原因。

```
Switch#show interfaces status err-disabled
Port      Name               Status       Reason
Gi1/0/2                      err-disabled gbic-invalid
Gi2/0/3                      err-disabled dtp-flap
```

【示例 15】显示 Catalyst 4500 系列交换机上模块 5 上所有接口的中继信息（注意，在 Catalyst 4500 系列交换机中这个命令不是直接集成在 **show interfaces** 命令中，而是以单独的 **show interfaces trunk** [**module** *mod*]命令进行的）。从中可以看出指定接口上的所有与中继相关的信息。

```
Switch#show interfaces trunk module 5

Port        Mode             Encapsulation  Status        Native vlan
Fa5/1       routed           negotiate      routed        1
Fa5/2       routed           negotiate      routed        1
Fa5/3       routed           negotiate      routed        1
Fa5/4       routed           negotiate      routed        1
Fa5/5       routed           negotiate      routed        1
Fa5/6       off              negotiate      not-trunking  10
Fa5/7       off              negotiate      not-trunking  10
Fa5/8       off              negotiate      not-trunking  1
Fa5/9       desirable        n-isl          trunking      1
Fa5/10      desirable        negotiate      not-trunking  1
Fa5/11      routed           negotiate      routed        1
Fa5/12      routed           negotiate      routed        1
...
Fa5/48      routed           negotiate      routed        1

Port        Vlans allowed on trunk
Fa5/1       none
Fa5/2       none
Fa5/3       none
Fa5/4       none
Fa5/5       none
Fa5/6       none
Fa5/7       none
Fa5/8       200
Fa5/9       1-1005
Fa5/10      none
Fa5/11      none
Fa5/12      none

Fa5/48      none

<……>
```


4.3.6　IOS 交换机 MAC 地址信息查看

在交换机的管理中，各以太网接口上所连接的网卡 MAC 地址查看是经常要进行的，如发现一个异常的 MAC 经常在网络内发送广播帧，或者在查找 ARP 攻击源时知道了这个源 MAC 地址，想查看是连接在交换机的哪个端口上。

在 Cisco IOS 交换机中为查看 MAC 地址列表配置了许多命令，但是不同系列交换机支持的命令不完全一样。而且以下命令**在 Catalyst 2950/2960/3650/3750 等非模块交换机系列中是在用户模式下执行的，而在 Catalyst 4000/4500/4900 等模块交换机系列中却只能在特权模式下执行**。

1．show mac address-table 命令

show mac address-table 用户模式命令仅适用于 Catalyst 2950/2960/3650/3750 等非模块交换机系列中，用来查看指定的静态和动态 MAC 地址列表。它在 12.2(25)FX、12.2(53)SE2 和 12.2(55)SE 等 IOS 版本中支持。该命令的完整格式如下：

```
show mac address-table [ | {begin | exclude | include} expression]
```

命令中的可选项和参数说明如下：

- | begin：（多选一选项）显示自第一个包括参数 *expression* 表达式开始以后行的 MAC 地址列表。
- |exclude：（多选一选项）显示不包括参数 *expression* 表达式的行的 MAC 地址列表。
- |include：（多选一选项）显示包括参数 *expression* 表达式的行的 MAC 地址列表。

- *expression*：（可选项）设置一个用于限制显示 MAC 地址列表行的表达式，注意表达式是区分大小写的。

以下示例是显示当前交换机上保存的所有 MAC 地址列表，其中的 Ports 列显示的是对应 MAC 地址所属的端口。凡是显示 CPU 的则是交换机自身的静态 MAC 地址，在 Type 列此时显示为 STATIC。

```
Switch>show mac address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
 All    0000.0000.0001    STATIC      CPU
 All    0000.0000.0002    STATIC      CPU
 All    0000.0000.0003    STATIC      CPU
 All    0000.0000.0009    STATIC      CPU
 All    0000.0000.0012    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
   1    0030.9441.6327    DYNAMIC     Gi6/0/4
Total Mac Addresses for this criterion: 12
```

2．show mac address-table address 命令

show mac address-table address 命令可以显示指定 MAC 地址的 MAC 地址列表信息。在 Catalyst 2950/2960/3650/3750 等非模块交换机系列中，该命令的格式为：

```
show mac address-table address mac-address [interface interface-id] [vlan vlan-id] [ | {begin | exclude | include} expression]
```

在 Catalyst 4000/4500/4900 等模块交换机系列中的命令格式为：

```
show mac-address-table address mac_addr [interface type slot/port | protocol protocol | vlan vlan_id]
```

以上两种命令格式中的可选项和参数说明如下：

- *mac-address*：指定要显示 MAC 地址列表的 48 位 MAC 地址，有效格式为 H.H.H（4 段十六进制格式）。
- interface *interface-id*：（可选项）指定要显示接口 MAC 地址列表的接口 ID。
- vlan *vlan-id*：（可选项）指定要显示 MAC 列表信息的 VLAN，*vlan-id* 的取值范围为 1～4094。如果指定 VLAN 不存在，则显示所有 VLAN 中的 MAC 地址列表。
- **protocol** *protocol*：（可选项）指定显示用于特定协议的 MAC 地址列表，可选项包括 ip、ipx、assigned、other（其他协议）协议。
- | begin：（多选一选项）显示自第一个包括参数 *expression* 表达式开始以后行的 MAC 地址列表。
- | exclude：（多选一选项）显示不包括参数 *expression* 表达式的行的 MAC 地址列表。
- | include：（多选一选项）显示包括参数 *expression* 表达式的行的 MAC 地址列表。
- *expression*：（可选项）设置一个用于限制显示 MAC 地址列表行的表达式，注意表达式是区分大小写的。

show mac-address-table address 命令在 12.2(55)SE、12.2(54)SG、12.2(53)SE2、12.2(25)FX、12.1(8a)EW、12.1(12c)EW 和 12.2(25)EW 等 IOS 版本中得到支持。想要查看某个 MAC 地址属于哪个交换机端口时就可以使用该命令。

以下示例显示了与 0002.4b28.c482 相关的 MAC 地址列表。

```
Switch#show mac address-table address 0002.4b28.c482
          Mac Address Table
-------------------------------------------
```

```
Vlan       Mac Address       Type        Ports
----       -----------       ----        -----
 All       0002.4b28.c482    STATIC    CPU
Total Mac Addresses for this criterion: 1
```

3．show mac address-table aging-time 命令

show mac address-table aging-time 命令用来显示指定 MAC 地址列表老化时间。在 Catalyst 2950/2960/3650/3750 等非模块交换机系列中，该命令的格式为：

```
show mac address-table aging-time [vlan vlan-id] [ | {begin | exclude | include} expression]
```

在 Catalyst 4000/4500/4900 等模块交换机系列中的命令格式为：

```
show mac-address-table aging-time [vlan vlan_id]
```

以上两种命令格式中的可选项和参数说明如下：

- vlan *vlan-id*：（可选）显示指定 VLAN 的 MAC 地址列表老化时间，*vlan-id* 的取值范围为 1～4094。如果指定 VLAN 不存在，则显示所有 VLAN 中的 MAC 地址表老化时间。
- | begin：（多选一选项）显示自第一个包括参数 *expression* 表达式开始以后行的 MAC 地址列表老化时间。
- | exclude：（多选一选项）显示不包括参数 *expression* 表达式的行的 MAC 地址列表老化时间。
- | include：（多选一选项）显示包括参数 *expression* 表达式的行的 MAC 地址列表老化时间。
- *expression*：（可选项）设置一个用于限制显示 MAC 地址列表老化时间行的表达式，注意表达式是区分大小写的。

show mac address-table aging-time 命令在 12.2(55)SE、12.2(54)SG、12.2(53)SE2、12.2(25)FX、12.1(8a)EW、12.1(12c)EW 等 IOS 版本中得到支持。想要查看每个接口存在多长时间时就可以使用该命令，特别是 VLAN 接口，从中可以得出这个 VLAN 是什么时间创建的。

以下示例是显示交换机所有 MAC 地址列表的老化时间。在输出信息中列出了 3 个 VLAN 中的 MAC 地址列表老化时间分别为 300 秒、300 秒和 400 秒。

```
Switch>show mac address-table aging-time
Vlan       Aging Time
----       ----------
1           300
2           300
3           400
```

以下示例是显示 VLAN 10 中的 MAC 地址列表老化时间。在输出信息中列出了 VLAN 10 中的 MAC 地址列表老化时间为 300 秒。

```
Switch>show mac address-table aging-time vlan 10
Vlan       Aging Time
----       ----------
  10        300
```

4．show mac address-table count 命令

show mac address-table count 命令用来显示当前在所有 VLAN 或者指定 VLAN 中的 MAC 地址数。在 Catalyst 2950/2960/3650/3750 等非模块交换机系列中，该命令的格式为：

```
show mac address-table count [vlan vlan-id] [ | {begin | exclude | include} expression]
```

在 Catalyst 4000/4500/4900 等模块交换机系列中的命令格式为：

```
show mac-address-table count [vlan vlan_id]
```

以上两种命令格式中的可选项和参数说明如下：

- vlan *vlan-id*：（可选）显示指定 VLAN 的 MAC 地址数，*vlan-id* 的取值范围为 1～4094。如果指定 VLAN 不存在，则显示所有 VLAN 中的 MAC 地址数。
- | begin：（多选一选项）显示自第一个包括参数 *expression* 表达式开始以后行的 MAC 地址数。
- | exclude：（多选一选项）显示不包括参数 *expression* 表达式的行的 MAC 地址数。

- | include：（多选一选项）显示包括参数 *expression* 表达式的行的 MAC 地址数。
- *expression*：（可选项）设置一个用于限制显示 MAC 地址数的行的表达式，注意表达式是区分大小写的。

show mac address-table count 命令在 12.2(55)SE、12.2(54)SG、12.2(53)SE2、12.2(25)FX、12.1(8a)EW、12.1(12c)EW 等 IOS 版本中得到支持。想要查看交换机 MAC 地址列表中有多少个 MAC 地址时可以使用该命令。

以下示例是显示所有 VLAN 中的 MAC 地址数。输出信息中显示了 VLAN 1 中有两条动态 MAC 地址。

```
Switch#show mac address-table count
Mac Entries for Vlan     : 1
---------------------------
Dynamic Address Count    : 2
Static   Address Count   : 0
Total Mac Addresses      : 2
```

5．show mac address-table dynamic 命令

show mac address-table dynamic 命令用来仅显示 MAC 地址列表中的动态 MAC 地址条目。在 Catalyst 2950/2960/3650/3750 等非模块交换机系列中，该命令的格式为：

```
show mac address-table dynamic [address mac-address] [interface interface-id] [vlan vlan-id] [ | {begin | exclude | include} expression]
```

在 Catalyst 4000/4500/4900 等模块交换机系列中的命令格式为：

```
show mac-address-table dynamic [address mac_addr | interface type slot/port | protocol protocol | vlan vlan_id]
```

以上两种命令格式中的可选项和参数说明如下：

- *mac-address*：指定要显示 MAC 地址列表的 48 位 MAC 地址，有效格式为 H.H.H（4 段十六进制格式）。注意，**在 Catalyst 2950/2960/3650/3750 等非模块交换机系列中，该参数仅可在特权模式下执行。**
- interface *interface-id*：（可选项）指定要显示动态 MAC 地址条目的接口 ID。
- vlan *vlan-id*：（可选项）指定要显示动态 MAC 地址条目信息的 VLAN，*vlan-id* 的取值范围为 1～4094。如果指定 VLAN 不存在，则显示所有 VLAN 中的动态 MAC 地址条目。
- **protocol** *protocol*：（可选项）指定显示用于特定协议的动态 MAC 地址条目，可选项包括 ip、ipx、assigned、other（其他协议）协议。
- | begin：（多选一选项）显示自第一个包括参数 *expression* 表达式开始以后行的动态 MAC 地址条目。
- | exclude：（多选一选项）显示不包括参数 *expression* 表达式的行的动态 MAC 地址条目。
- | include：（多选一选项）显示包括参数 *expression* 表达式的行的动态 MAC 地址条目。
- *expression*：（可选项）设置一个用于限制显示动态 MAC 地址条目行的表达式，注意表达式是区分大小写的。

show mac address-table dynamic 命令在 12.2(55)SE、12.2(54)SG、12.2(53)SE2、12.2(25)FX、12.1(8a)EW、12.1(12c)EW 和 12.2(25)EW 等 IOS 版本中得到支持。想要查看交换机上各接口所学习到的 MAC 地址时就可以使用该命令。

以下示例是显示交换机上所有 VLAN 中的动态 MAC 地址条目。从输出信息中可以看出每个端口所学习的 MAC 地址。

```
Switch#show mac-address-table dynamic
Unicast Entries
 vlan    mac address       type            protocols                 port
-------+---------------+--------+---------------------+--------------------
   1     0000.0000.0201    dynamic ip                    FastEthernet6/15
   1     0000.0000.0202    dynamic ip                    FastEthernet6/15
   1     0000.0000.0203    dynamic ip,assigned           FastEthernet6/15
```

```
   1    0000.0000.0204    dynamic ip,assigned          FastEthernet6/15
   1    0000.0000.0205    dynamic ip,assigned          FastEthernet6/15
   2    0000.0000.0101    dynamic ip                   FastEthernet6/16
   2    0000.0000.0102    dynamic ip                   FastEthernet6/16
   2    0000.0000.0103    dynamic ip,assigned          FastEthernet6/16
   2    0000.0000.0104    dynamic ip,assigned          FastEthernet6/16
   2    0000.0000.0105    dynamic ip,assigned          FastEthernet6/16
Switch#
```

6．show mac address-table static 命令

show mac address-table static 命令用来仅显示 MAC 地址列表中的静态 MAC 条目。在 Catalyst 2950/2960/3650/3750 等非模块交换机系列中，该命令的格式为：

```
show mac address-table static [address mac-address] [interface interface-id] [vlan vlan-id] [ | {begin | exclude | include} expression]
```

在 Catalyst 4000/4500/4900 等模块交换机系列中的命令格式为：

```
show mac-address-table static [address mac_addr | interface type number | protocol protocol | vlan vlan_id]
```

以上两种命令格式中的可选项和参数说明如下：

- *mac-address*：指定要显示 MAC 地址列表的 48 位 MAC 地址，有效格式为 H.H.H（4 段十六进制格式）。注意，**在 Catalyst 2950/2960/3650/3750 等非模块交换机系列中，该参数仅可在特权模式下执行。**
- interface *interface-id*：（可选项）指定要显示静态 MAC 地址条目的接口 ID。
- vlan *vlan-id*：（可选项）指定要显示静态 MAC 地址条目信息的 VLAN，*vlan-id* 的取值范围为 1～4094。如果指定 VLAN 不存在，则显示所有 VLAN 中的静态 MAC 地址条目。
- **protocol** *protocol*：（可选项）指定显示用于特定协议的静态 MAC 地址条目，可选项包括 ip、ipx、assigned、other（其他协议）协议。
- | begin：（多选一选项）显示自第一个包括参数 *expression* 表达式开始以后行的静态 MAC 地址条目。
- | exclude：（多选一选项）显示不包括参数 *expression* 表达式的行的静态 MAC 地址条目。
- | include：（多选一选项）显示包括参数 *expression* 表达式的行的静态 MAC 地址条目。
- *expression*：（可选项）设置一个用于限制显示静态 MAC 地址条目行的表达式，注意表达式是区分大小写的。

show mac address-table static 命令在 12.2(55)SE、12.2(54)SG、12.2(53)SE2、12.1(8a)EW、12.1(12c)EW 和 12.2(25)EW 等 IOS 版本中得到支持。

以下示例是显示交换机上的所有静态 MAC 地址条目。输出信息中分单播（Unicast）和组播（Multicast）MAC 地址条目列出。组播 MAC 地址均为 ffff.ffff.ffff。

```
Switch#show mac-address-table static
Unicast Entries
 vlan    mac address       type            protocols                 port
-------+---------------+--------+---------------------+--------------------
   1     0030.94fc.0dff    static ip,ipx,assigned,other  Switch
Fa6/1    0030.94fc.0dff    static ip,ipx,assigned,other  Switch
Fa6/2    0030.94fc.0dff    static ip,ipx,assigned,other  Switch

Multicast Entries
 vlan     mac address       type      ports
-------+---------------+-------+-------------------------------------------
   1     ffff.ffff.ffff    system Switch,Fa6/15
   2     ffff.ffff.ffff    system Fa6/16
1002     ffff.ffff.ffff    system
1003     ffff.ffff.ffff    system
1004     ffff.ffff.ffff    system
1005     ffff.ffff.ffff    system
```

```
Fa6/1     ffff.ffff.ffff     system Switch,Fa6/1
Fa6/2     ffff.ffff.ffff     system Switch,Fa6/2
.
.
Switch#
```

7．show mac address-table interface 命令

show mac address-table interface 命令用来显示指定 VLAN 中指定接口的 MAC 地址列表信息。在 Catalyst 2950/2960/3650/3750 等非模块交换机系列中，该命令的格式为：

```
show mac address-table interface interface-id [vlan vlan-id] [ | {begin | exclude | include} expression]
```

在 Catalyst 4000/4500/4900 等模块交换机系列中的命令格式为：

```
show mac-address-table interface type slot/port
```

以上两种命令格式中的可选项和参数说明如下：

- interface *interface-id*：指定要显示接口 MAC 地址列表的接口 ID。
- **interface** *type slot/port*：指定要显示接口 MAC 地址列表的接口类型/插槽号/端口号。
- vlan *vlan-id*：（可选项）指定要显示 MAC 地址列表信息的 VLAN，*vlan-id* 的取值范围为 1～4094。如果指定 VLAN 不存在，则显示所有 VLAN 中的 MAC 地址列表。
- **protocol** *protocol*：（可选项）指定显示用于特定协议的 MAC 地址列表，可选项包括 ip、ipx、assigned、other（其他协议）协议。
- | begin：（多选一选项）显示自第一个包括参数 *expression* 表达式开始以后行的 MAC 地址列表。
- | exclude：（多选一选项）显示不包括参数 *expression* 表达式的行的 MAC 地址列表。
- | include：（多选一选项）显示包括参数 *expression* 表达式的行的 MAC 地址列表。
- *expression*：（可选项）设置一个用于限制显示 MAC 地址列表行的表达式，注意表达式是区分大小写的。

show mac address-table interface 命令在 12.2(55)SE、12.2(54)SG、12.2(53)SE2、12.2(25)FX、12.1(8a)EW、12.1(12c)EW 等 IOS 版本中得到支持。

以下示例是显示 fastethernet6/16 接口上的 MAC 地址列表信息。输出信息中分单播（Unicast）和组播（Multicast）MAC 地址条目列出。从中可以看出，该接口学习到了许多 MAC 地址，这是由于在该接口上更改了多次所连接的网络设备。组播 MAC 地址均为 ffff.ffff.ffff。

```
Switch#show mac-address-table interface fastethernet6/16
Unicast Entries
 vlan     mac address        type            protocols                  port
-------+---------------+--------+---------------------+--------------------
    2     0000.0000.0101     dynamic other                FastEthernet6/16
    2     0000.0000.0102     dynamic other                FastEthernet6/16
    2     0000.0000.0103     dynamic other                FastEthernet6/16
    2     0000.0000.0104     dynamic other                FastEthernet6/16
    2     0000.0000.0105     dynamic other                FastEthernet6/16
    2     0000.0000.0106     dynamic other                FastEthernet6/16

Multicast Entries
 vlan      mac address        type       ports
-------+---------------+-------+-----------------------------------------------
    2     ffff.ffff.ffff     system Fa6/16
Switch#
```

8．show mac address-table learning 命令

使用 **show mac address-table learning** 命令显示所有 VLAN 或者指定 VLAN 的 MAC 地址动态学习状态。使用不带任何关键字的 **show mac address-table learning** 命令可以显示配置的 VLAN，不管它们的 MAC 地址学习功能是启用的还是禁止的。默认在所有 VLAN 上都是启用

MAC 地址动态学习功能的。使用带指定 VLAN_ID 的该命令可以显示特定 VLAN 的 MAC 地址动态学习功能状态。

该命令在 Catalyst 2950/2960/3650/3750 等非模块交换机系列和在 Catalyst 4000/4500/4900 等模块交换机系列的命令格式均为：

show mac address-table learning [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

该命令的可选项和参数说明如下：

- vlan *vlan-id*：（可选项）指定要显示动态 MAC 地址学习状态的 VLAN，*vlan-id* 的取值范围为 1～4094。如果指定 VLAN 不存在，则显示所有 VLAN 中的动态 MAC 地址学习功能状态。
- | begin：（多选一选项）显示自第一个包括参数 *expression* 表达式开始以后行的动态 MAC 地址学习功能状态列表。
- | exclude：（多选一选项）显示不包括参数 *expression* 表达式的行的动态 MAC 地址学习功能状态列表。
- | include：（多选一选项）显示包括参数 *expression* 表达式的行的动态 MAC 地址学习功能状态列表。
- *expression*：设置一个用于限制显示动态 MAC 地址学习功能状态列表行的表达式，注意表达式是区分大小写的。

show mac address-table learning 命令在 12.2(55)SE、12.2(54)SG、12.2(53)SE2 和 12.2(25)FX 等 IOS 版本中得到支持。

以下示例是显示交换机各 VLAN 的 MAC 地址动态学习功能状态。从输出信息中可以看出 VLAN 1、VLAN 100 的 MAC 地址动态学习功能是开启的，而 VLAN 200 的 MAC 地址动态学习功能是禁止的。

```
Switch>show mac address-table learning
VLAN      Learning Status
----      ---------------
1                 yes
100               yes
200               no
```

9．show mac address-table notification 命令

show mac address-table notification 命令用来显示交换机上所有接口或者指定接口上的 MAC 地址改变通知设置。使用不带任何选项的 **show mac address-table notification** 命令可查看交换机上各接口的 MAC 地址改变通知功能设置、发送通知的时间间隔、允许保留的最大 MAC 地址改变通知条数和历史通知内容。使用带有 **interface** 关键字的该命令可以查看所有接口或者指定接口上的以上信息。

在 Catalyst 2950/2960/3650/3750 等非模块交换机系列中，该命令的格式为：

show mac address-table notification {**change** [**interface** [*interface-id*] | **mac-move** | **threshold**} [| {**begin** | **exclude** | **include**} *expression*]

在 Catalyst 4000/4500/4900 等模块交换机系列中的命令格式为：

show mac-address-table notification [change] [interface [*interface-id***]] | [mac-move] | [threshold] | [learn-fail]**

以上两种命令格式中的可选项和参数说明如下：

- change：显示 MAC 地址更改通知功能和通知历史列表。
- interface：（可选项）显示所有接口上的 MAC 地址通知功能信息，包括物理接口和以太网通道接口。
- *interface-id*：（可选项）显示指定接口上的 MAC 地址通知功能信息，包括物理接口和以太网通道接口。
- mac-move：显示 MAC 地址移去通知功能状态。

- threshold：显示 MAC 地址列表阈值监控状态。
- learn-fail：（可选项）显示 MAC 地址学习失败所产生的信息。仅在 12.2(52)SG IOS 版本中支持。
- | begin：（多选一选项）显示自第一个包括参数 *expression* 表达式开始以后行的 MAC 地址改变、移去或学习失败的通知信息。
- | exclude：（多选一选项）显示不包括参数 *expression* 表达式的行的 MAC 地址改变、移去或学习失败的通知信息。
- | include：（多选一选项）显示包括参数 *expression* 表达式的行的 MAC 地址改变、移去或学习失败的通知信息。
- *expression*：（可选项）设置一个用于限制显示 MAC 地址改变、移去或学习失败的通知信息行的表达式，注意表达式是区分大小写的。

show mac-address-table notification 命令在 12.2(55)SE、12.2(54)SG、12.2(53)SE2、12.2(52)SG、12.2(31)SG 和 12.2(25)FX 等 IOS 版本中得到支持。

以下示例是显示交换机上所有的 MAC 地址改变通知信息。从输出信息中可以得知交换机中 MAC 地址通知功能的设置状态、发送通知的时间间隔、新添加的 MAC 地址数、移去的 MAC 地址数、所配置的 MAC 地址通知的最大条目数、当前历史 MAC 通知列表长度，以及发生变化的各 MAC 地址信息。

```
Switch>show mac address-table notification change
MAC Notification Feature is Enabled on the switch
Interval between Notification Traps : 60 secs
Number of MAC Addresses Added : 4
Number of MAC Addresses Removed : 4
Number of Notifications sent to NMS : 3
Maximum Number of entries configured in History Table : 100
Current History Table Length : 3
MAC Notification Traps are Enabled
History Table contents
----------------------
History Index 0, Entry Timestamp 1032254, Despatch Timestamp 1032254
MAC Changed Message :
Operation: Added     Vlan: 2        MAC Addr: 0000.0000.0001 Module: 0     Port: 1

History Index 1, Entry Timestamp 1038254, Despatch Timestamp 1038254
MAC Changed Message :
Operation: Added     Vlan: 2        MAC Addr: 0000.0000.0000 Module: 0     Port: 1
Operation: Added     Vlan: 2        MAC Addr: 0000.0000.0002 Module: 0     Port: 1
Operation: Added     Vlan: 2        MAC Addr: 0000.0000.0003 Module: 0     Port: 1

History Index 2, Entry Timestamp 1074254, Despatch Timestamp 1074254
MAC Changed Message :
Operation: Deleted Vlan: 2        MAC Addr: 0000.0000.0000 Module: 0     Port: 1
Operation: Deleted Vlan: 2        MAC Addr: 0000.0000.0001 Module: 0     Port: 1
Operation: Deleted Vlan: 2        MAC Addr: 0000.0000.0002 Module: 0     Port: 1
Operation: Deleted Vlan: 2        MAC Addr: 0000.0000.0003 Module: 0     Port: 1
```

10．show mac address-table vlan 命令

show mac address-table vlan 命令用来显示指定 VLAN 中的 MAC 地址列表信息。在 Catalyst 2950/2960/3650/3750 等非模块交换机系列中，该命令的格式为：

```
show mac address-table vlan vlan-id [ | {begin | exclude | include} expression]
```

在 Catalyst 4000/4500/4900 等模块交换机系列中的命令格式为：

```
show mac-address-table [vlan vlan_id] [protocol protocol]
```

以上两种命令格式中的可选项和参数说明如下：

- vlan *vlan-id*：（可选项）指定要显示 MAC 地址列表的 VLAN，*vlan-id* 的取值范围为 1～4094。如果指定 VLAN 不存在，则显示所有 VLAN 中的 MAC 地址列表。
- **protocol** *protocol*：（可选项）指定显示用于特定协议的 MAC 地址列表，可选项包括 ip、ipx、assigned、other（其他协议）协议。
- | begin：（多选一选项）显示自第一个包括参数 *expression* 表达式开始以后行的 MAC 地址列表。
- |exclude：（多选一选项）显示不包括参数 *expression* 表达式的行的 MAC 地址列表。
- |include：（多选一选项）显示包括参数 *expression* 表达式的行的 MAC 地址列表。
- *expression*：（可选项）设置一个用于限制显示 MAC 地址列表行的表达式，注意表达式是区分大小写的。

show mac address-table vlan 命令在 12.2(55)SE、12.2(54)SG、12.2(53)SE2、12.1(8a)EW、12.1(8a)EW 和 12.1(12c)EW 等 IOS 版本中得到支持。

以下示例是显示 VLAN 1 中的 MAC 地址列表。输出信息中分单播（Unicast）和组播（Multicast）MAC 地址两类。组播 MAC 地址均为 ffff.ffff.ffff。

```
Switch#show mac-address-table vlan 1
Unicast Entries
 vlan    mac address       type            protocols                 port
-------+---------------+--------+---------------------+--------------------
    1    0000.0000.0201    dynamic ip                              FastEthernet6/15
    1    0000.0000.0202    dynamic ip                              FastEthernet6/15
    1    0000.0000.0203    dynamic other                           FastEthernet6/15
    1    0000.0000.0204    dynamic other                           FastEthernet6/15
    1    0030.94fc.0dff    static ip,ipx,assigned,other    Switch

Multicast Entries
 vlan    mac address       type       ports
-------+---------------+-------+-----------------------------------------------
    1    ffff.ffff.ffff    system Switch,Fa6/15
Switch#
```

4.4　Cisco IOS 交换机二层接口模式配置

每个二层以太网端口可以连接到一个单一工作站或服务器，或者通过一个集线器把工作站或服务器连接到网络。典型的以太网集线器中，所有端口都与集线器中的公共背板连接，连接到集线器中的所有设备共享网络带宽。如果两个站点建立会话时使用了较高的带宽，则网络连接到该集线器中的其他站点可能需要降低连接性能，甚至无法连接。为了减少这种性能的降低，交换机则把每个 LAN 端口视为一个虚拟网段。当连接到不同 LAN 端口的站点需要通信时，交换机可以以线速把帧从一个端口转发到另一个端口上，以确保每个会话可以使用全部的带宽。

为了使不同 LAN 端口的帧交换更加有效，交换机还维护着一个二层的 MAC 地址列表。当一个帧进入到交换机时，交换机将把发送帧的网络设备的 MAC 地址与交换机的 LAN 端口进行关联，以确定是由哪个端口来接收。一般来说，在 Cisco 交换机中可以存储至少 32000 个 MAC 地址。交换机可以使用老化机制（它是由定时器定义的），在某个 MAC 地址条目处于非活动状态达到了指定的限期时将其从列表中删除，以维护交换机的 MAC 地址列表不过于庞大，从而不影响查询效率。

要配置二层以太网接口，首先要把对应接口转换成二层模式（参见 4.2.1 节）。表 4-7 列出了 Cisco IOS 交换机的二层接口模式转换命令及相应的功能描述。各种二层模式的配置方法将在下面各小节中介绍。

表 4-7　Cisco IOS 交换机的二层接口模式命令

二层接口模式设置命令	用途说明
switchport mode access	转换为 **access**（访问）模式。 使接口置于永久非中继模式，协商转换链路为非中继链路。把接口转换为非 Trunk 端口，即使邻居接口不发生改变
switchport mode dynamic desirable	转换为 **dynamic desirable**（动态适应）模式。 使接口主动试图转换链路为中继链路。如果邻居接口设置为 **trunk**、**desirable** 或 **auto** 模式，则接口转换为中继接口
switchport mode dynamic auto	转换为 **dynamic auto**（动态自动）模式。 如果邻居接口设置为 **trunk** 或 **desirable** 模式，则把接口转换成中继链路。对于所有以太网接口来说，这是一种默认模式
switchport mode trunk	转换为 **trunk**（中继）模式。 使接口置于永久中继模式，协商转换链路为中继链路。把接口转换为 Trunk 端口，即使邻居接口不发生改变
switchport nonegotiate	转换为 **nonegotiate**（非协商）模式。 使接口置于永久中继模式，但阻止接口产生 DTP 帧。必须手动配置邻居接口作为中继接口，以建立中继链路
switchport mode dot1q-tunnel	转换为 **dot1q-tunnel**（IEEE 802.1Q 隧道封装）模式。 使接口置于 dot1q 隧道（非中继）模式。配置接口作为非对称链路中的 Tunnel 端口，用于与 IEEE 802.1QTrunk 端口连接。IEEE 802.1Q 隧道用于维护 ISP 网络客户端 VLAN 的完整性

4.4.1　配置二层以太网接口为 Access 端口

在 Cisco IOS 交换机中二层以太网接口都是交换端口（Switch Port）。交换端口包括 Access 端口（Access Port）、Trunk 端口（Trunk Port）和 Tunnel 端口（Tunnel Port）3 种。本节及后面几个小节将分别介绍 Access 端口、Trunk 端口及其相关配置。本节介绍的是二层 Access 端口的配置方法。

一个 Access 端口仅可属于并且承载一个 VLAN 内的通信（除非被配置成语音 VLAN 端口），一般用于连接计算机。Access 端口上接收和发送的通信是不带 VLAN 标记的本地格式，到达一个 Access 端口的通信是假定来自分配到该端口的 VLAN。

【注意】如果分配一个接口到一个不存在的 VLAN 中，接口将不工作，直到在 VLAN 数据库中建立该 VLAN。

可以按照 4-8 所示的步骤为二层 Access 端口配置接口（自特权模式开始）。

表 4-8　为二层 Access 端口配置接口的步骤

步骤	命令	用途说明
1	Switch(config)#**interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port*	指定要配置的接口，进入接口配置模式
2	Switch(config-if)#**shutdown**	（可选）关闭接口以阻止通信流，直到配置完成
3	Switch(config-if)#**switchport**	（可选）转换该接口为二层交换接口。在可以键入带有关键字的 **switchport** 命令之前必须键入一次不带任何参数的 **switchport** 命令，以配置接口作为二层端口。仅在以前为该接口键入了 **no switchport** 命令把该接口转换成了三层接口时才需要
4	Switch(config-if)#**switchport mode access**	配置接口作为二层 Access 端口。如果不执行本步操作，则仅把接口配置为二层交换端口。 12.1(12c)EW、12.1(13)EW、12.2(25)FX、12.2(53)SE2、12.2(54)SG 和 12.2(55)SE 等大多数 IOS 版本均支持该命令
5	Switch(config-if)#**switchport access vlan** *vlan_id*	（可选）把接口置于一个静态 VLAN 中，取值范围为 1～4094。如果仅需要把接口配置为交换端口，则不需要执行此步。 12.1(12c)EW、12.1(13)EW、12.2(25)FX、12.2(53)SE2、12.2(54)SG 和 12.2(55)SE 等大多数 IOS 版本均支持该命令
6	Switch(config-if)#**no shutdown**	激活接口（仅在接口处于关闭状态时需要）
7	Switch(config-if)#**end**	退出接口配置模式
8	Switch#**show running-config interface** {**fastethernet** | **gigabitethernet**} *slot/port*	显示在运行配置中的指定接口配置
9	Switch#**show interfaces** [{**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port*] **switchport**	显示指定接口的交换端口配置

Switchport 接口配置模式命令在 Catalyst 3650/3750 系列交换机（如运行 12.2(53)SE2、12.2(55)SE IOS 版本的这些系列交换机）中是没有任何可选项和参数的（实际上是有的，只是它们是以独立命令出现的），但在 Catalyst 4000/4500/4900 系列交换机中（如运行 12.1(8a)EW、12.1(11)EW 和 12.2(54)SG IOS 版本的这些系列交换机）的命令格式如下：

```
Switchport [access vlan vlan_num] | [nonegotiate] | [voice vlan {vlan_id | dot1p | none | untagged}]
```

在 Catalyst 4000/4500/4900 系列交换机中，该命令除了把对应接口转换成二层交换端口外，还可以用来编辑交换端口特性配置。在 Catalyst 2950/2960 系列中不支持该命令。要取消原来的二层交换端口特性配置，则可用 **no switchport [access | nonegotiate | voice vlan]** 命令。

- access vlan *vlan_num*：（可选项）当接口为二层访问模式时，设置接口所属的 VLAN，有效的 vlan_id 范围是 1～1005。
- nonegotiate：（可选项）指定该接口为非协商模式，不能在该接口上发送 DISL/DTP（动态 ISL/动态中继协议）协议帧。
- voice vlan *vlan_id*：（可选项）设置该二层交换接口所属语音 VLAN，有效的 vlan_id 范围是 1～1005。
- dot1p：（可选项）指定该接口优先使用标记的 PVID（端口 VLAN ID）帧。
- none：（可选项）指定在该接口上不能进行电话和语音通信。
- untagged：（可选项）指定该接口使用非标记的 PVID 帧。

【示例 1】把工作在可路由模式的以太网接口转换为二层交换端口。

```
Switch(config-if)#switchport
Switch(config-if)#
```

【示例 2】把以太网接口设置为二层 Access 端口，并分配其属于 VLAN 2。

```
Switch(config-if)#switchport access vlan 2
Switch(config-if)#
```

【示例 3】把处于中继协商模式的接口转换成中继或访问模式端口（具体要依据该接口上使用 **switchport mode** 命令的设置而定）。

```
Switch(config-if)#switchport nonegotiate
Switch(config-if)#
```

【示例 4】把该接口添加到语音 VLAN 2 中。

```
Switch(config-if)#switchport voice vlan 2
switchport voice vlan 2
Switch(config-if)#
```

【示例 5】配置 Fast Ethernet interface 5/6 作为 VLAN 200 的 Access 端口。

```
Switch#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)#interface fastethernet 5/6
Switch(config-if)#shutdown
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 200
Switch(config-if)#no shutdown
Switch(config-if)#end
Switch#exit
```

【示例 6】校验运行配置中的指定接口配置。

```
Switch#show running-config interface fastethernet 5/6
Building configuration...
!
Current configuration :33 bytes
interface FastEthernet 5/6
 switchport access vlan 200
 switchport mode access
end
```

【示例 7】校验交换机指定接口的端口配置。

```
Switch#show running-config interface fastethernet 5/6 switchport
Name:Fa5/6
Switchport:Enabled
Administrative Mode:dynamic auto
Operational Mode:static access
Administrative Trunking Encapsulation:negotiate
Operational Trunking Encapsulation:native
Negotiation of Trunking:On
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Administrative private-vlan host-association:none
Administrative private-vlan mapping:none
Operational private-vlan:none
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001
Switch#
```


4.4.2 配置以太网接口为二层 Trunk 端口

中继是在一个或多个以太网交换接口和其他网络设备（如路由器或交换机）之间的点对点链路。中继模式允许属于不同 VLAN 的数据帧都可以通过中继链路传输数据帧。有关 Trunk 端口模式请参见 4.2.1 节。

1．Trunk 模式类型

可以在单一以太网接口或以太网通道上配置中继模式。以太网中继接口支持不同的中继模式，具体如表 4-9 所示。可以指定使用 ISL 或 802.1Q 封装，或者通信双方自动协商（Negotiate）封装方式。中继协商是由 DTP（Dynamic Trunking Protocol，动态中继协议）管理的。DTP 支持 ISL 和 802.1Q 两种封装的协商。

表 4-9 以太网中继封装类型

封装类型	封装命令	用途说明
ISL	**switchport trunk encapsulation isl**	指定在中继链路采用 ISL 封装类型
802.1Q	**switchport trunk encapsulation dot1q**	指定在中继链路采用 802.1Q 封装类型
Negotiate	**switchport trunk encapsulation negotiate**	指定接口与邻居接口协商封装类型，协商的依据是配置、邻居接口性能等

要配置成自动协商中继模式，必须确保接口在同一个 VTP（VLAN Trunking Protocol，VLAN 中继协议）域（有关 VTP 方面的具体知识将在第 8 章介绍）中。使用 **trunk** 或 **nonegotiate** 关键字可以强制不同域的接口中继。通信中的两个相邻接口的中继模式、中继封装类型和硬件性能决定了是采用 ISL 还是 802.1Q 中继模式。

Trunk 端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的数据帧，一般用于交换机间的连接。二层接口默认是 **dynamic auto** 模式（动态自动模式，具体解释参见表 4-8 中的 **switchport mode** 命令介绍）。如果邻居接口支持中继（Trunk），并且配置为 **trunk** 或 **dynamic desirable** 模式，则链路将成为二层中继链路，而且默认是采用中继封装类型协商方式；如果邻居接口支持 ISL 和 802.1Q 封装类型，且两个接口都设置为封装类型协商模式，则链路使用 ISL 封装类型。但是 Supervisor Engine 6-E 不支持 ISL 封装。

【说明】完成本小节的各种配置前，必须先完成 4.4.1 节第 1 小点中介绍的通过 **switchport** 命令把以太网接口配置成交换端口的步骤。

2．配置一个以太网接口作为二层 Trunk 端口

配置二层中继的步骤如表 4-10 所示（自特权模式开始）。

表 4-10　配置二层中继的步骤

步骤	命令	用途说明
1	Switch(config)#**interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port*	指定要配置的接口，进入接口配置模式
2	Switch(config-if)#**shutdown**	（可选）关闭接口以阻止通信流，直到配置完成
3	Switch(config-if)#**switchport trunk encapsulation** {**isl** | **dot1q** | **negotiate**}	（可选）指定封装类型。必须在此命令中键入 **isl** 或 **dot1q** 关键字，以支持下一步的 **switchport mode trunk** 命令，因为默认的 **negotiate**（协商）模式是不支持下一步的 **switchport mode trunk** 命令的
4	Switch(config-if)#**switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**}	配置接口作为二层中继（仅当接口是作为二层 Access 端口或者指定中继模式时才需要）
5	Switch(config-if)#**switchport access vlan** *vlan_id*	（可选）指定访问 VLAN，在接口停止中继时使用。访问 VLAN 不能用作本地 VLAN。 参数 *vlan_id* 要么是一个范围为 1～1005 的单独 VLAN ID 或者以逗号分隔的多个单独 VLAN，要么是一个由两个 VLAN ID 指定的范围，中间以连接号连接。但在两个以逗号分隔的 VLAN 或者以破折号连接的两个 VLAN 之间不要键入任何空格
6	Switch(config-if)#**switchport trunk native vlan** *vlan_id*	对于 802.1Q 中继类型，指定本地 VLAN，此 VLAN 的 ID 作为 PVID 值。如果不指定本地 VLAN，则默认是使用 VLAN 1 作为本地 VLAN
7	Switch(config-if)#**switchport trunk allowed vlan** {**add** | **except** | **all** |**remove**} *vlan_id*[,*vlan_id*[,*vlan_id*[,....]]	（可选）配置允许中继的 VLAN 列表。默认是所有 VLAN 都可以中继。不能从中继中删除任何默认 VLAN
8	Switch(config-if)#**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan_id*[,*vlan_id*[,*vlan_id*[,....]]	（可选）配置在中继中有资格修剪的 VLAN 列表。默认所有 VLAN 都具有修剪资格，除了 VLAN 1 外
9	Switch(config-if)#**no shutdown**	激活接口（仅在接口处于关闭状态时需要）
10	Switch(config-if)#**end**	退出接口配置模式
11	Switch#**show running-config interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port*	显示在运行配置中的指定接口配置
12	Switch#**show interfaces** [**fastethernet** | **gigabitethernet** | **tengigabitethernet**] *slot/port* **switchport**	显示指定接口的交换端口配置
13	Switch#**show interfaces** [{**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port*] **trunk**	显示指定接口的中继配置

【示例 1】配置 fastethernet 5/8 接口 802.1Q 中继，中继模式为 dynamic desirable（动态适应）。示例中假设邻居接口已配置支持 802.1Q 中继，本地 VLAN 默认为 VLAN 1。

```
Switch#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)#interface fastethernet 5/8
Switch(config-if)#shutdown
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode dynamic desirable
Switch(config-if)#no shutdown
Switch(config-if)#end
Switch#exit
```

【示例 2】校验运行配置中的 fastethernet 5/8 接口的配置（主要目的就是查看前面所做的中继配置是否成功，注意输出信息中的粗体字部分）。

```
Switch#show running-config interface fastethernet 5/8
Building configuration...
Current configuration:
!
interface FastEthernet5/8
 switchport mode dynamic desirable
 switchport trunk encapsulation dot1q
end
```

【示例 3】校验 fastethernet 5/8 接口的交换端口配置。

```
Switch#show interfaces fastethernet 5/8 switchport
Name: Fa5/8
Switchport: Enabled
Administrative Mode: dynamic desirable
```

```
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Enabled
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

【示例 4】校验 fastethernet 5/8 接口的中继配置。

```
Switch#show interfaces fastethernet 5/8 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa5/8       desirable    n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa5/8 1-1005

Port        Vlans allowed and active in management domain
Fa5/8 1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005

Port        Vlans in spanning tree forwarding state and not pruned
Fa5/8 1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005

Switch#
```

3．配置二层中继使用 DTP

Cisco DTP 是 VLAN 协议组中 Cisco 的专有协议，主要用于协商两台设备间链路上的中继模式及中继封装（如 ISL 或 802.1Q）类型。如果一个端口可以成为 Trunk 端口，那么该端口也可能具有自动中继功能，在某些情况下，甚至具有协商哪种中继类型的功能。这种与其他设备之间进行的协商中继方法的过程被称为动态中继技术。

可以配置二层接口使用 DTP，配置二层接口使用 DTP 的命令如表 4-11 所示。

表 4-11　配置二层中继使用 DTP 的命令

命令	用途说明
Switch(config-if)#**switchport mode dynamic {auto | desirable}**	（可选）配置中继接口使用 DTP
Switch(config-if)#**no switchport mode**	恢复中继接口到默认的中继模式（动态交换模式）

【注意】在配置了二层中继使用 DTP 后，仅当接口是二层访问或者指定了中继模式时才需要使用 DTP。

4．配置二层中继不使用 DTP

配置二层中继不使用 DTP 的步骤如表 4-12 所示。

表 4-12　配置二层中继不使用 DTP 的步骤

步骤	命令	用途说明
1	Router(config-if)#**switchport mode trunk**	（可选）配置端口无条件地中继
	Router(config-if)#**no switchport mode**	恢复到默认的中继模式（使用 dynamic desirable 交换模式）
2	Router(config-if)#**switchport nonegotiate**	（可选）配置中继不使用 DTP
	Router(config-if)#**no switchport nonegotiate**	在端口上启用 DTP

在配置二层中继不使用 DTP 时，应注意以下事项：

- 在键入 **switchport mode trunk** 命令前必须配置封装方式，参见本节第 2 小点。

- 要支持 **switchport nonegotiate** 命令，必须键入 **switchport mode trunk** 命令。
- 需要键入 **switchport mode dynamic trunk** 命令。
- 在键入 **switchport nonegotiate** 命令前必须配置封装方式，参见本节第 2 小点；并且配置端口使用 **switchport mode trunk** 命令无条件地中继，参见本小节第 3 小点。

5．配置 802.1Q 本地 VLAN

本地 VLAN（Native VLAN）是 IEEE 802.1Q 中的概念，是一个不带标记（Tag）的 VLAN，主要用于管理，默认为 VLAN 1。配置本地 VLAN 的命令为 **switchport trunk native vlan** *vlan_ID*，*vlan_ID* 参数的取值范围也为 1～4094。如果指定的 VLAN 是锁定的，则可以使用 VLAN 名替代 VLAN 号。访问 VLAN 不自动用于本地 VLAN。

6．校验二层中继配置

想要查看二层中继配置，可以使用表 4-13 所列的命令。

表 4-13　查看二层中继配置的命令

命令	用途说明
Router#**show running-config interface** *type slot/port*	显示指定接口上当前运行的配置
Router#**show interfaces** [*type slot/port*] **switchport**	显示指定接口上的交换端口配置
Router#**show interfaces** [*type slot/port*] **trunk**	显示指定接口上的中继配置

下面是一个显示如何把 Catalyst 6500 系列交换机上的 Fa5/8 接口配置成 802.1Q Trunk 端口（假设其邻接端口也是配置成支持 802.1Q 中继的），并校验该接口的配置的示例。

```
Router#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Router(config)#interface fastethernet 5/8
Router(config-if)#shutdown
Router(config-if)#switchport
Router(config-if)#switchport mode dynamic desirable
Router(config-if)#switchport trunk encapsulation dot1q
Router(config-if)#no shutdown
Router(config-if)#end
Router#exit

Router#show running-config interface fastethernet 5/8
Building configuration...
Current configuration:
!
interface FastEthernet5/8
 no ip address
 switchport
 switchport trunk encapsulation dot1q
end

Router#show interfaces fastethernet 5/8 switchport
Name: Fa5/8
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Enabled
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: ALL
```

```
Router#show interfaces fastethernet 5/8 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa5/8       desirable    n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa5/8 1-1005

Port        Vlans allowed and active in management domain
Fa5/8 1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005

Port        Vlans in spanning tree forwarding state and not pruned
Fa5/8 1-6,10,20,50,100,152,200,300,303-305,349-351,400,500,521,524,570,801-8
02,850,917,999,1002-1005

Router#
```


4.4.3 清除 IOS 交换机中的二层接口配置

按照表 4-14 所示的步骤清除接口的二层属性配置（自特权模式开始）。

表 4-14 清除接口的二层配置的步骤

步骤	命令	用途说明
1	Switch(config)#**default interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port*	清除指定接口的二层配置，恢复成默认设置
2	Switch(config-if)#**end**	退出接口配置模式
3	Switch#**show running-config interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port*	显示运行配置中的指定接口配置
4	Switch#**show interfaces** [{**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port*] **switchport**	显示指定接口的交换端口配置

【示例 1】清除 Fast Ethernet interface 5/6 接口上的二层配置。

```
Switch#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)#default interface fastethernet 5/6
Switch(config)#end
Switch#exit
```

【示例 2】校验指定接口的运行配置。

```
Switch#show running-config interface fastethernet 5/6
Building configuration...
Current configuration:
!
interface FastEthernet5/6
end
```

【示例 3】校验指定接口的交换端口配置。

```
Switch#show interfaces fastethernet 5/6 switchport
Name: Fa5/6
Switchport: Enabled
Switch#
```

4.5 Cisco IOS 交换机以太网接口属性配置

本节介绍的 Cisco IOS 交换机以太网接口的基本属性配置同时适用于二层以太网接口和三层以太网接口，其中主要配置的属性包括：接口速率、双工模式、流量控制、Auto-MDIX 等。

4.5.1　IOS 交换机以太网接口的默认属性

在 Cisco IOS 交换机中，所有以太网接口都有默认的二层属性配置。要使用某特征时，就一定要注意这些接口上的默认设置，否则就很难确定是否需要对这些二层以太网接口属性进行改变。

表 4-15 显示了 Cisco IOS 交换机以太网接口的一些主要二层属性默认配置，但是要注意，**不同交换机系列，以太网接口的默认属性设置也可能不一样**。表中显示的是 Catalyst 3750 系列交换机的以太网接口默认属性设置。

表 4-15　Catalyst 3750 系列交换机以太网接口的默认属性设置

特征	默认值
接口模式	二层交换模式
中继封装	协商封装类型
许可 VLAN 范围	VLAN 1～4094
Access 端口默认的 VLAN	VLAN 1
802.1Q 中继的本地 VLAN	VLAN 1
VLAN 中继	交换模式为动态自动模式（Dynamic Auto）
端口启用状态	全部启用
端口描述	没有定义
端口速率	自动协商（Autonegotiate）
双工模式	自动协商（Autonegotiate）
流量控制	接收方向流量控制关闭，发送方向流量控制总是关闭的
以太网通道（PAgP）	在所有以太网端口上禁止以太网通道
端口阻塞	二层以太网端口禁止端口阻塞
多播、广播和单播控制	禁止
端口保护（Protected Port）	二层以太网端口禁止
端口安全（Port Security）	二层以太网端口禁止
端口快速（Port Fast）	禁止
Auto-MDIX	启用
PoE	启用
STP 协议	在所有 VLAN 上启用
STP 端口优先权	128
STP 端口开销	10Mb/s 以太网 LAN 端口开销为 100；10/100Mb/s 快速以太网 LAN 端口开销为 19；100Mb/s 快速以太网 LAN 端口开销为 19；1000Mb/s 快速以太网 LAN 端口开销为 4；10000Mb/s 快速以太网 LAN 端口开销为 2

4.5.2　IOS 交换机以太网接口描述配置

默认情况下，Cisco Catalyst 以太网交换机的接口是没有定义描述的。可以为一些特殊用户的接口（如连接关键服务器或者关键网络设备的接口）添加一个描述，以便在进行交换机管理时能快速地识别这些特殊的接口状态。接口描述会在 **show configuration**、**show running-config** 和 **show interfaces** 特权模式命令的输出中显示。

为以太网接口添加描述的配置步骤如表 4-16 所示（从特权模式开始）。

表 4-16　为接口添加描述的步骤

步骤	命令	用途说明
1	Switch#**configure terminal**	进入全局配置模式
2	Switch(config)#**interface** *interface-id*	指定要添加描述的接口并进入接口配置模式
3	Switch(config-if)#**description** *string*	为接口添加描述（最多 240 个字符）
4	Switch(config-if)#**end**	返回到特权模式

续表

步骤	命令	用途说明
5	Switch#**show interfaces** *interface-id* **description** 或者 Switch#**show running-config**	校验以上接口描述配置
6	Switch#**copy running-config startup-config**	（可选）在配置文件中保存设置更改

可以使用 **no description** 接口配置命令删除描述。

以下示例是配置 gigabitethernet1/0/2 接口描述为“Connects to Marketing”，然后通过 **show interfaces** 命令验证该接口所配置的描述（注意输出信息中的粗体字部分）。

```
Switch#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gigabitethernet1/0/2
Switch(config-if)#description Connects to Marketing
Switch(config-if)#end
Switch#show interfaces gigabitethernet1/0/2 description
Interface Status                Protocol Description
Gi1/0/2   admin down            down        Connects to Marketing
```


4.5.3 IOS 交换机以太网接口速率和双工模式配置

一般情况下是不需要设置以太网接口速率和双工模式的，只需要按照默认的设置即可，但当这个以太网接口连接与对端接口不一致的情况下，就需要考虑为接口重新设置速率的双工模式了，以达到最佳的通信效果。例如你当前这个以太网接口是 10/100/1000Mb/s 的，而对端是 10/100Mb/s 的，这时你可能就要把当前的以太网接口速率设置成 10Mb/s 或 100Mb/s，以达到速率匹配。

在 Cisco IOS 交换机中，以太网接口速率是通过 **speed** {**10** | **100** | **1000** | **auto** [**10** | **100** | **1000**] | **nonegotiate**} 接口配置模式命令进行配置的，双工模式是通过 **duplex** {**auto** | **full** | **half**} 接口配置命令进行配置的。IOS 交换机的以太网接口速率和双工模式的具体配置步骤如表 4-17 所示。

表 4-17　设置接口速率和双工模式的步骤

步骤	命令	用途说明
1	Switch#**configure terminal**	进入全局配置模式
2	Switch(config)#**interface** *interface-id*	指定要配置的物理接口，进入接口配置模式
3	Switch(config-if)#**speed** {**10**	**100**	**1000**	**auto** [**10**	**100**	**1000**]	**nonegotiate**}	为以太网接口设置速率，但此命令不能在 10G 以太网接口上使用 ● 10：多选一选项，配置以太网接口工作在 10Mb/s 速率 ● 100：多选一选项，配置以太网接口工作在 100Mb/s 速率 ● 1000：多选一选项，配置以太网接口工作在 1000Mb/s 速率 ● auto 10	100	1000：多选一选项，指定让对应以太网接口与对端设备接口进行速率自动协商，可以是一个具体的速率值，如 10Mb/s、100Mb/s 或 1000Mb/s，也可以是两个速率的选择，如 10Mb/s 或 100Mb/s、100Mb/s 或 1000Mb/s 等 ● nonegotiate：多选一选项，设置对应以太网接口不与对端设备接口协商速率 默认选择的是 **auto** 选项。可以用 **no speed** 接口配置命令删除对应接口上的速率配置，恢复为默认设置
4	Switch(config-if)#**duplex** {**auto**	**full**	**half**}	为以太网接口指定双工模式，但此命令不能在 10G 以太网接口上使用 ● auto：多选一选项，启用自动双工模式配置，这时以太网接口就会依据所连接的对端设备双工模式来自动工作在全双工或者半双工模式 ● full：多选一选项，把对应以太网接口设置为全双工模式 ● half：多选一选项，把对应以太网接口设置为半双工模式。但只能为工作在 10Mb/s 或 100Mb/s 速率的以太网接口配置半双工模式，而不能为工作在 1000Mb/s 或 10000Mb/s 速率的以太网接口配置半双工模式 对于快速以太网接口默认选择的是 **half** 选项，千兆以太网接口默认选择的是 **auto** 选项。可以用 **no duplex** 接口配置模式命令取消对应以太网接口上的双工模式配置，恢复为默认设置

续表

步骤	命令	用途说明
5	Switch(config-if)#**end**	返回到特权模式
6	Switch#**show interfaces** *interface-id*	显示接口速率和双工配置
7	Switch#**copy running-config startup-config**	（可选）在配置文件中保存设置更改

在配置接口速率（Speed）和双工（Duplex）模式时，需要注意以下事项：

- 10/100Mb/s 快速以太网端口支持以下 **speed** 配置命令中除 1000Mb/s 选项以外的速率和双工选项。
- 10/100/1000Mb/s 千兆以太网端口支持以下 **speed** 配置命令中所有速率和所有双工选项（auto（自动）、half（半双工）和 full（全双工）），但是仅工作在 1000Mb/s 的千兆以太网端口不支持半双工模式。
- 不能为 10G 以太网端口配置速率和双工模式，因为这种接口仅可以工作在 10000Mb/s 速率和全双工模式下。
- SFP 模块端口，速率和双工选项依据 SFP 模块类型而定：
  - 1000BASE-*x*（*-x* 是指-BX、-CWDM（Coarse Wavelength-Division Multiplexing，类波分复用）、-LX、-SX 和-ZX）类型的 SFP 模块端口在速率配置中支持 **nonegotiate**（不协商）关键字，但不支持双工配置选项。
  - 1000BASE-T 类型的 SFP 模块端口与 10/100/1000Mb/s 端口支持相同的速率和双工选项。
  - 100BASE-*x*（*-x* 是指-BX、-CWDM、-LX、-SX 和-ZX）类型的 SFP 模块端口仅支持 100Mb/s 速率。这些模块支持全双工和半双工选项，但是不支持 **autonegotiation**（自动协商）选项。
- 对于在交换机上支持哪种 SFP 模块，可以看产品说明书。如果通信线路两端都支持自动协商，建议默认设置为 **auto**（自动协商）；如果通信线路两端中的一个端口支持自动协商，而另一个端口不支持自动协商，则需要在双方端口上进行速率和双工配置，不要在支持自动协商的一端使用 **auto** 选项进行设置。

以上注意事项可用表 4-18 来概括。

表 4-18　各种类型以太网接口所支持的速率和双工模式设置命令格式

接口类型	支持的命令语法格式	默认设置	说明
10/100Mb/s 双绞线以太网接口	**speed** [**10** | **100** | **auto** [**10** | **100**]] **duplex** [**half** | **full**]	**auto** **half**	如果速率设置为自动协商，则你不能为该以太网接口设置双工模式。 如果该以太网接口速率设置为 10Mb/s 或 100Mb/s，而且你又没有配置双工模式，则双工模式为默认的半双工模式
100Mb/s 光纤模块接口	不支持接口速率配置命令 **duplex** [**half** | **full**]	没有默认速率设置 **half**	这类光纤以太网接口速率总是为 1000Mb/s
Gigabit 双绞线以太网接口	**speed nonegotiate** 不支持双工模式设置命令	**Nonegotiate** 没有默认设置	可选项仅适用于双绞线千兆以太网接口，仅支持全双工模式
10/100/1000Mb/s 双绞线以太网接口	**speed** [**10** | **100** | **1000** | **auto** [**10** | **100** | **1000**]] **duplex** [**half** | **full**]	**auto**	如果该以太网接口速率设置为 10Mb/s 或 100Mb/s，而且你又没有为该接口配置双工模式，则该接口为默认的半双工模式；如果该接口速率设置为 1000Mb/s 或者自动协商，则你不能设置该接口为半双工模式
1000Mb/s 光纤以太网接口	不支持接口速率和双工模式设置命令	没有默认设置	这类光纤以太网接口速率总是为 1000Mb/s，而且仅是半双工模式

【注意】改变接口速率和双工模式配置可能会在配置过程中先关闭接口，然后重新启用接口。

以太网接口速率和双工模式的设置彼此影响，设置时一定要注意。表 4-19 所示的是几种设置组合的最终结果。

表 4-19　以太网接口速率和双工模式命令设置相互影响的几种特例

双工模式设置命令	速率设置命令	最终结果
duplex auto	**speed auto**	以太网接口速率和双工模式都自动协商
duplex half	**speed 10**	强制接口速率为 10Mb/s，双工模式为半双工
duplex full	**speed 10**	强制接口速率为 10Mb/s，双工模式为全双工
duplex half	**speed 100**	强制接口速率为 100Mb/s，双工模式为半双工
duplex full	**speed 100**	强制接口速率为 100Mb/s，双工模式为全双工
duplex full	**speed 1000**	强制接口速率为 1000Mb/s，双工模式为全双工

下面是几个以太网接口速率和双工模式设置的示例。

【示例 1】设置一个 10/100Mb/s 快速以太网端口的速率为 10Mb/s，双工模式为半双工。

```
Switch#configure terminal
Switch(config)#interface fasttethernet 1/1
Switch(config-if)#speed 10
Switch(config-if)#duplex half
```

【示例 2】设置一个 10/100/1000Mb/s 千兆以太网接口的速率为 100Mb/s，双工模式为全双工。

```
Switch#configure terminal
Switch(config)#interface gigabitethernet1/10
Switch(config-if)#speed 100
Switch(config-if)#duplex full
```

【示例 3】设置一个 10/100/1000Mb/s 千兆以太网接口的速率为自动协商 10Mb/s 或 100Mb/s，双工模式为全双工。

```
Switch#configure terminal
Switch(config)#interface gigabitethernet 1/0/1
Switch(config-if)#speed auto 10 100
Switch(config-if)#duplex full
```

【示例 4】设置一个 10/100/1000Mb/s 千兆以太网接口的速率为自动协商 100Mb/s。

```
Switch(config)#interface gigabitethernet 1/1
Switch(config-if)#speed auto 100
```

4.5.4　IOS 交换机以太网接口的流控制配置

IOS 交换机的流控制功能可以使连接的以太网端口在出现拥塞时通过允许拥塞节点暂停通信链路另一端的操作来控制通信流传输速率。如果一个端口出现了拥塞，而不能再接收任何更多的通信流，它将发送暂停帧到其他端口，停止发送数据帧到该端口，直到拥塞解除。在收到暂停帧后，发送设备停止发送任何数据帧，以免在拥塞期间出现任何数据帧的丢失。这里所说的“流控制”并非真正意义上的“流量控制”，因为它只是在“忙”时阻止对端接口继续发送数据帧，而不是控制接口上的流量大小。如果用句通俗的话来说，就是你在用 QQ 时，不时有人来打扰，跟你聊天，而你此时却忙不过来一一回复，这时你就可能会对对方说“我现在很忙，请稍后再说”，或者把 QQ 设置成“忙碌”状态，这样对方就不会再继续与你聊了。这里的“流控制”功能也是这样的意思。

【注意】有些交换机端口只能接收暂停帧，而不能发送暂停帧（也就是没有下面 **flowcontrol** 接口配置命令中的 send 关键字选项），如Catalyst 3750 及以前系列的交换机，而 Catalyst 4000/4500/4900/6500 等系列交换机中支持。

可以用 **flowcontrol** {**receive** | **send**} {**off** | **on** | **desired**}接口配置命令来设置接口是否可以接收或者发送暂停帧。IOS 交换机上以太网接口流控制功能的具体设置步骤如表 4-20 所示（从特权模式开始）。

【说明】可以使用不带任何选项的 **flowcontrol** 接口配置命令查看流控制命令设置详情和在本地、远程端口的控制效果。

表 4-21 描述了使用不同的 **send** 和 **receive** 关键字的流控制配置的含义。

表 4-20　流控制设置步骤

步骤	命令	用途说明
1	Switch#**configure terminal**	进入全局配置模式
2	Switch(config)#**interface** *interface-id*	指定要配置的物理接口并进入接口配置模式
3	Switch(config-if)#**flowcontrol** {**receive** | **send**} {**off** | **on** | **desired**}	为端口配置流控制模式。其中的可选项说明如下： ● receive：二选一选项，指定该以太网接口可以接收远程的流控制帧（也就是暂停帧） ● send：二选一选项，指定该以太网接口可以发送暂停帧，但在 Cisco Catalyst 3750 及以前系列中不支持 ● off：多选一选项，禁止该以太网接口接收和处理来自对端接口的暂停帧，或禁止发送暂停帧 ● on：多选一选项，允许该以太网接口接收和处理来自对端接口的暂停，或允许发送暂停帧 ● desired：多选一选项，让该以太网接口自动与对端接口协商，以获取最佳效果
4	Switch(config-if)#**end**	返回到特权模式
5	Switch#**show interfaces** *interface-id*	校验接口的流控制设置
6	Switch#**copy running-config startup-config**	（可选）在配置文件中保存设置更改

表 4-21　不同流控制设置的含义

配置	说明
send on	允许本地以太网接口发送暂停帧。要获得好的效果，仅当对端接口设置为 **receive on** 或 **receive desired** 时才在本接口上设置
send off	禁止本地以太网接口发送暂停帧。要获得好的效果，仅当对端接口设置为 **receive off** 或 **receive desired** 时才在本接口上设置
send desired	与对端接口的 **receive on**、**receive off** 或 **receive desired** 设置协商
receive on	允许本地以太网接口接收暂停帧。仅当对端接口设置为 **send on** 或 **send desired** 时才在本接口上设置
receive off	禁止本地以太网接口接收暂停帧。仅当对端接口设置为 **receive off** 或 **receive desired** 时才在本接口上设置
receive desired	与对端接口的 **send on**、**send off** 或 **send desired** 设置协商

表 4-22 显示了在本地和远程端口上的不同流控制设置会出现的最终结果，可以在配置流控制时提供参考，千万别认为只要启用了流控制功能就可以达到你想要的目的了。

表 4-22　本地和远程端口上的流控制设置及最后的流控制结果

流控制设置		流控制结果	
本地端口	远程端口	本地端口	远程端口
send off/receive on	**send on/receive on**	仅接收暂停帧	可发送和接收暂停帧
	send on/receive off	仅接收暂停帧	仅可发送暂停帧
	send desired/receive on	仅接收暂停帧	可发送和接收暂停帧
	send desired/receive off	仅接收暂停帧	仅可发送暂停帧
	send off/receive on	仅接收暂停帧	仅可接收暂停帧
	send off/receive off	不能发送或不能接收暂停帧	不能发送或不能接收暂停帧
send off/receive off	**send on/receive on**	不能发送或不能接收暂停帧	不能发送或不能接收暂停帧
	send on/receive off	不能发送或不能接收暂停帧	不能发送或不能接收暂停帧
	send desired/receive on	不能发送或不能接收暂停帧	不能发送或不能接收暂停帧
	send desired/receive off	不能发送或不能接收暂停帧	不能发送或不能接收暂停帧
	send off/receive on	不能发送或不能接收暂停帧	不能发送或不能接收暂停帧
	send off/receive off	不能发送或不能接收暂停帧	不能发送或不能接收暂停帧

要取消原来的流控制设置，可以使用对应的 **no flowcontrol {receive | send} {off | on | desired}**接口配置命令。

【示例 1】在 gigabitethernet1/0/1 端口上启用接收流控制请求。

```
Switch#configure terminal
Switch(config)#interface gigabitethernet1/0/1
Switch(config-if)#flowcontrol receive on
Switch(config-if)#end
```

【示例 2】在 gigabitethernet1/0/1 端口上禁止发送流控制请求。

```
Switch#configure terminal
Switch(config)#interface gigabitethernet1/0/1
```

```
Switch(config-if)#flowcontrol send off
Switch(config-if)#end
```

【示例 3】在 gigabitethernet1/0/1 端口上启用流控制自动协商功能。

```
Switch#configure terminal
Switch(config)#interface gigabitethernet1/0/1
Switch(config-if)#flowcontrol receive desired
Switch(config-if)#end
```

4.5.5 IOS 交换机以太网接口的 Auto-MDIX 配置

我们知道这样一个双绞电缆选择原则：同种设备（如交换机通过普通以太网端口的互连）连接使用交叉电缆，而不同设备连接（如交换机和路由器或 PC 机的互连）则要用直通电缆。虽然只有两种选择，但有时也会给我们带来一些麻烦，因为现在在市场中购买的双绞电缆通常都是直通电缆，交叉电缆则需要自己来制作。以太网交换机上的这种 Auto-MDIX 功能就可以很好地解决这个问题，因为在交换机的以太网接口上启用 Auto-MDIX（Automatic Medium-Dependent Interface Crossover，自动媒体相关接口交叉）功能后，接口就能自动检测当前连接所需的电缆连接类型（直通线或交叉线），然后检测当前所使用的连接电缆，自动根据连接类型需求进行适当的配置。这样，你就可以随便使用什么类型的双绞电缆了。

IOS 交换机 Auto-MDIX 功能的配置是使用 **mdix auto** 接口配置模式命令进行的。在一些 Cisco 交换机（如 Cisco Catalyst 3650/3750/4500/4900 等系列）上是默认支持 Auto-MDIX 功能的，所以一般无需另外配置。可以用 **no mdix auto** 接口配置模式命令禁止 Auto-MDIX 功能。**在启用 Auto-MDIX 功能后，必须设置接口速率和双工模式为 auto（自动）**，以便接口能正确工作。如果你设置了 Auto-MDIX 功能，但在以太网接口速率和双工模式中设置成了协商模式，则链路将激活不了，除非你按传统标准使用了正确的电缆来连接。Auto-MDIX 在所有 10/100Mb/s 和 10/100/1000Mb/s 以太网接口，以及 10/100/1000BASE-TX SFP 模块接口上都是支持的，但在 1000BASE-SX/-LX SFP 模块接口上不支持。

在以太网接口上配置 Auto-MDIX 功能的步骤如表 4-23 所示（从特权模式开始）。

表 4-23 配置 Auto-MDIX 功能的步骤

步骤	命令	用途说明
1	Switch#**configure terminal**	进入全局配置模式
2	Switch(config)#**interface** *interface-id*	指定要配置的物理接口并进入接口配置模式
3	Switch(config-if)#**speed auto**	配置接口速率为自动协商
4	Switch(config-if)#**duplex auto**	配置接口双工模式也为自动协商
5	Switch(config-if)#**mdix auto**	在接口上启用 Auto-MDIX 功能
6	Switch(config-if)#**end**	返回到特权模式
7	Switch#**show controllers ethernet-controller** *interface-id* phy	校验接口上 Auto-MDIX 功能的工作状态
8	Switch#**copy running-config startup-config**	（可选）在配置文件中保存设置更改

表 4-24 所示为在本地以太网接口和远端以太网接口上设置 Auto-MDIX 功能后，使用正确和错误类型（是根据不同设备连接时电缆选择规则而言的）电缆时的链路状态结果。

表 4-24 不同 Auto-MDIX 设置的链路状态结果

本端 Auto-MDIX	远端 Auto-MDIX	正确电缆类型	错误电缆类型
On（启用）	On（启用）	Link up	Link up
On（启用）	Off（禁用）	Link up	Link up
Off（禁用）	On（启用）	Link up	Link up
Off（禁用）	Off（禁用）	Link up	Link down

从表中可以看出，链路两端只要有一端接口启用了 Auto-MDIX 功能，无论使用了正确类型的电缆还是错误类型的电缆，链路都将被激活。只有在链路两端的接口上均没有启用 Auto-MDIX 功

能，在使用了这种类型的电缆后链路才关闭，也就是不通。

以下示例显示了如何在一端口上启用自动速率匹配、自动双工模式选择，以及 Auto-MDIX 功能。

```
Switch#configure terminal
Switch(config)#interface gigabitethernet1/0/1
Switch(config-if)#speed auto
Switch(config-if)#duplex auto
Switch(config-if)#mdix auto
Switch(config-if)#end
```

4.5.6　IOS 交换机以太网接口 PoE 配置

PoE（Power over Enthernet）就是通过以太网电缆供电的意思，这在 4.2.7 节中已有介绍。PoE 主要应用于不太方便提供市电插座的情况下（用作中继或者级联的交换机，中间没有电源插座），目前 Cisco 的许多系列交换机都支持 PoE，如 Catalyst 2950/2960/3650/3750/4500/4900 等。在大多数情况下，支持 PoE 的交换机的默认配置（自动模式）可以很好地工作，提供即插即用，无须其他进一步的配置。但也可以使用以下配置为 PoE 端口配置更高的优先级，使该端口仅用于数据帧传输，或者指定允许的最高功能，以拒绝高电源功率设备连接在该端口上。

【注意】在改变 PoE 端口配置时，在配置过程中端口电源功率会降低。依据新的配置、PoE 端口状态和电源预算状态，端口可能不能再提供电源了。例如，端口 1 是工作在自动模式，并且处于正常工作中，而你又把它改变为静态模式，这时交换机就会从端口 1 上移出电源，检测电源设备来重新为端口提供电源。如果端口 1 设置成自动模式，并且正常工作，同时配置了一个最高 10W 的功率，则交换机从该端口上移出电源，然后检测电源设备。交换机仅在电源设备为 1、2 类型或者 Cisco 品牌的电源设备时重新为该端口 1 供电。

可以按照表 4-25 所示的步骤配置 PoE 端口上的电源管理模式（自特权模式开始）。

表 4-25　配置 PoE 端口上的电源管理模式的步骤

步骤	命令	用途说明
1	Switch#**configure terminal**	进入全局配置模式
2	Switch(config)#**interface** *interface-id*	指定要配置的接口并进入接口配置模式
3	**Cisco Catalyst 4500/4900 等系列：** Switch(config-if)#**power inline** {**auto** [**max** *milliwatt*] | **never** | **static** [**max** *milliwatt*] | **consumption** *milliwatt*} 可以用 **no power inline** 命令取消原来的 PoE 模式设置 **Cisco Catalyst 3650/3750 等系列：** Switch(config-if)#**power inline** {**auto** [**max** *max-wattage*] | **never** | **police** [**action** {**errdisable** | **log**}] | **port priority** {**high** | **low**}] | **static** [**max** *max-wattage*]} 可以用 **no power inline** {**auto** | **never** | **police** | **port priority**| **static**}命令取消原来的 PoE 模式设置 **Cisco Catalyst 2950/2960 等系列：** Switch(config-if)#**power inline** {**auto** [**max** *max-wattage*] | **never** | **police** [**action log**] | **static** [**max** *max-wattage*]}	在端口上配置 PoE 模式，可以有如下几个选项（注意选项所对应的交换机系列）： ● **auto**：将支持 PoE 功能的以太网接口设置为 PoE 自动模式 ● **max** *milliwatt*：（可选）设置可分配给设备的最大电力，Catalyst 4500/4900 等系列交换机底盘模块的最大可分配电力范围为 2000mW～15400mW，WS-X4648-RJ45V-E 模块的最大可分配电力为 20000mW，WS-X4648-RJ45V+E 模块的最大可分配电力为 30000mW ● **max** *max-wattage*：（可选）为 Catalyst 3650/3750 等系列交换机设置可分配的最大电力，取值范围为 4000mW～30000mW，如果不指定最大值，则可以允许最大电力 30000mW ● **never**：禁止 PoE 检测和电力分配 ● **police**：为 Catalyst 2950/2960/3650/3750 等系列交换机启用实时电力分配策略，可以用 **power inline police** [**action** {**errdisable** | **log**}] 接口配置模式命令配置电力分配策略。如果选择 **action errdisable** 选项，则当实时分配的电力超过了该端口所能承受的最大电力时，把该端口的电源关闭，这是默认行为；如果选择的是 **action log** 选项，则当实时分配的电力超过了该端口所能承受的最大电力时，持续为该端口供电，并在交换机上生成一个系统日志 ● **port priority** {**high** | **low**}：为堆叠电源端口配置电力分配优先级，如果电力供应失效，则低优先级的端口首先将关闭电源。默认为低（low）优先级 ● **static**：恒定地为设备分配电力 **power inline** 命令在 12.1(11)EW、12.1(19)EW、12.1(20)EW、12.2(44)SG、12.2(44)SE、12.2(46)SE、12.2(53)SE2 等多个 IOS 版本中得到支持。在交换机为自动模式配置的端口分配电源前，交换机会先为静态模式配置的端口分配电源

续表

步骤	命令	用途说明
4	Switch(config-if)#**end**	返回到特权模式
5	Switch#**show power inline** [*interface-id* | module *switch-number*]	显示交换机或交换机堆叠上指定接口或者指定堆叠成员的 PoE 状态
6	Switch#**copy running-config startup-config**	（可选）在配置文件中保存配置更改

【说明】使用 **max** *max-wattage* 选项可以使交换机拒绝为需要比 *max-wattage* 参数设置值更高功率的设备提供电源。这样，当电源设备发送 CDP（Cisco 发现协议）消息请求比 *max-wattage* 参数设置的更高功率的电源时，则交换机关闭该端口的电源。如果遵守 802.3af 标准类别的电源设备提供的电力大于 *max-wattage* 参数所设置的最大功率，则交换机不再为该设备提供电源。

如果你在不支持 PoE 的以太网端口配置该命令，则会出现如下所示的命令错误提示：

```
Switch(config)#interface gigabitethernet1/0/1
Switch(config-if)#power inline auto
                  ^
% Invalid input detected at '^' marker.
```

或

```
Power over Ethernet not supported on interface Admin
```

【示例 1】在交换机 fastethernet 4/1 以太网接口上启用 PoE 自动检测和电力分配功能。

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastethernet 4/1
Switch(config-if)#power inline auto
Switch(config-if)#end
```

【示例 2】禁止交换机 fastethernet 4/1 以太网接口的 PoE 自动检测和电力分配功能。

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastethernet 4/1
Switch(config-if)#power inline never
Switch(config-if)#end
```

【示例 3】在交换机 fastethernet 4/1 以太网接口上分配恒定的 8000mW 电力，不管所连接的是 802.3af 标准类别的设备还是收到了请求电力的 CDP 帧。

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastethernet 4/1
Switch(config-if)#power inline consumption 8000
Switch(config-if)#end
```

【示例 4】在交换机 fastethernet 4/1 以太网接口上分配恒定的最大电力为 16500mW，不管所连接的是 802.3af 标准类别的设备还是收到了请求电力的 CDP 帧。

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gigabitethernet 2/1
Switch(config-if)#power inline static max 16500
Switch(config-if)#end
```

【示例 5】在交换机 gigabitethernet1/0/2 以太网接口上设置端口优先级为高，这样当电源失效时它将是最后一个关闭的端口。

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gigabitethernet1/0/2
Switch(config-if)#power inline port priority high
Switch(config-if)#end
```

4.5.7　IOS 交换机以太网接口链路状态和中继状态事件配置

在 Cisco IOS 交换机中可以使用 **logging event** 命令配置以太网接口的链路状态和中继状态事件日志功能，这样方便我们在需要时通过事件日志的查看了解相应接口的链路状态和中继状态历史。**logging event** 命令在 12.2(25)SG、12.2(53)SE2、12.2(25)FX 等多个 IOS 版本中得到支持。

在 Catalyst 2950/2960/3650/3750 等系列交换机上配置链路状态或中继状态事件日志的命令格式为：**logging event {link-status | trunk status}**，可以用 **no logging event { link-status | trunk status}**命令禁止链路状态（选择 **link-status** 选项时，下同）或中继状态（选择 **trunk status** 选项时，下同）事件日志功能。默认情况下，以太网接口的事件日志功能是禁止的。

在 Catalyst 4000/4500/4900 等系列交换机上链路状态或中继状态事件日志可以在全局和接口上分别配置，在全局配置模式下的配置命令为：**logging event** {**link-status global** | **trunk-status global**}，可以把事件日志配置应用到交换机的所有接口上，要取消原来的设置，则可以用 **no logging event** {**link-status global** | **trunk-status global** }全局配置模式命令；在接口配置模式下的配置命令为 **logging event** {**link-status** | **trunk-status**}，该事件日志设置仅应用到相应接口，要取消原来的设置，则可以用 **no logging event** {**link-status** | **trunk-status**}；还可以使用 **logging event** { **link-status** | **trunk-status**} **use-global** 接口配置模式命令在接口上应用全局配置的链路状态或中继状态事件日志设置。默认情况下，交换机的全局事件日志功能是启用的，但以太网接口的事件日志是禁止的。

【注意】在 Catalyst 4000/4500/4900 等系列交换机中，如果在交换机接口的链路状态或中继状态日志配置与全局设置不一样，则最终接口的状态配置是以接口上的配置为准。如果接口上启用了链路状态日志，而交换机的全局设置为禁用，则最终接口的链路状态日志事件为启用；同样，如果接口上禁用了链路状态日志，而交换机的全局设置为启用，则最终接口的链路状态日志事件为禁用。

以下显示了在配置了不同全局和接口日志设置时接口日志事件运行状态的摘要。其中“全局设置”列显示的是全局链路状态设置，而在“接口设置”列中显示的是接口链路状态设置，“实际日志状态”列显示的是接口最终实际运行的链路状态。

```
全局设置          接口设置              实际日志状态
--------------    ------------------    --------------------
     on           on                         on
     off          on                         on
     on           off                        off
     off          off                        off
     on           default(use-global)        on
     off          default(use-global)        off
```

【示例 1】在当前交换机上全局启用链路状态事件日志功能（仅适用于 Catalyst 4000/4500/4900 等系列交换机）。

```
Switch#config terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)#logging event link-status global
Switch(config)#end
Switch#
```

【示例 2】在当前交换机 gigabitethernet1/0/2 接口上启用链路状态事件日志功能。

```
Switch#config terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)#interface gigabitethernet1/0/2
Switch(config-if)#logging event link-status
Switch(config-if)#end
Switch#
```

【示例 3】在当前交换机 gigabitethernet1/0/2 上禁用链路状态事件日志功能，采用全局链路状

态事件日志设置（仅适用于 Catalyst 4000/4500/4900 等系列交换机）。

```
Switch#config terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)#interface gigabitethernet1/0/2
Switch(config-if)#no logging event link-status
Switch(config-if)#end
Switch#
```

【示例 4】在当前交换机 gigabitethernet1/0/2 上启用全局配置的链路状态事件日志功能设置（仅适用于 Catalyst 4000/4500/4900 等系列交换机）。

```
Switch#config terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)#interface gigabitethernet1/0/2
Switch(config-if)#logging event link-status use-global
Switch(config-if)#end
Switch#
```

【示例 5】在当前交换机上全局启用中继状态事件日志功能（仅适用于 Catalyst 4000/4500/4900 等系列交换机）。

```
Switch#config terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)#logging event trunk-status global
Switch(config)#end
Switch#
```

【示例 6】在当前交换机 gigabitethernet1/0/2 上启用中继状态事件日志功能。

```
Switch#config terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)#interface gigabitethernet1/0/2
Switch(config-if)#logging event trunk-status
Switch(config-if)#end
Switch#
```

【示例 7】在当前交换机 gigabitethernet1/0/2 上禁用中继状态事件日志功能，采用全局中继状态事件日志设置（仅适用于 Catalyst 4000/4500/4900 等系列交换机）。

```
Switch#config terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)#interface gigabitethernet1/0/2
Switch(config-if)#no logging event trunk-status
Switch(config-if)#end
Switch#
```

【示例 8】在当前交换机 gigabitethernet1/0/2 上启用全局配置的中继状态事件日志功能设置（仅适用于 Catalyst 4000/4500/4900 等系列交换机）。

```
Switch#config terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)#interface gigabitethernet1/0/2
Switch(config-if)#logging event trunk-status use-global
Switch(config-if)#end
Switch#
```

4.6 Cisco IOS 交换机 Tunnel 端口及配置

在本章前面已经介绍到，Cisco IOS 交换机中有一种称之为 Tunnel 端口的二层交换端口。它所利用的就是隧道（Tunneling）技术，是服务商为在他们的网络上承载多个客户通信而设计的一种功能，以便在不影响其他客户通信的情况下为每个客户维护 VLAN 和二层协议配置。但在 LAN Base 特性集的 IOS 系统中不支持IEEE 802.1Q 和二层协议隧道。

4.6.1　理解 IEEE 802.1Q Tunneling 技术

隧道技术是与 VLAN 紧密关联的，是在对应的 IEEE 802.1Q 标准中定义的。在具体的 ISP 服务中，服务商的商业客户在 VLAN ID 和 VLAN 数目方面时常有一些具体要求。同一服务商的不同客户所需的 VLAN 范围可能重叠，这样在同一基础架构中的不同用户的通信就会混在一起。如果为不同客户分配一个不同的 VLAN ID 范围，则又会对客户有所限制，而且很容易超出交换机上可创建的 VLAN ID 范围。

使用 IEEE 802.1Q 隧道功能，服务商可以使用单个 VLAN 来支持多个需要多个 VLAN 的客户。客户 VLAN ID 是受保护的，同一服务商的不同客户的通信是相互隔离的，即使他们看似处于同一个 VLAN 中。使用 IEEE 802.1Q 隧道功能的 VLAN-in-VLAN 分层结构（也就是用一个服务商提供的外部 VLAN 代表一个客户的多个内部 VLAN）和重标记已标记的数据包方案扩展了 VLAN 的空间。支持 IEEE 802.1Q 隧道功能的端口称为隧道端口（Tunnel Port）。当你配置隧道时，你指派一个隧道端口到在隧道中使用的 VLAN ID。每个客户需要一个独立的服务商 VLAN ID 作为外部 VLAN，但是这个 VLAN ID 支持所有客户自己的内部 VLAN。

来自客户端设备 IEEE 802.1Q 中继端口的客户通信先使用适当的 VLAN ID 进行标记，然后进入服务商边缘交换机上的 IEEE 802.1Q 隧道端口。客户端设备和服务商边缘设备上的链路是不对称的，因为一端是配置作为 IEEE 802.1Q 中继端口，另一端是被配置为隧道端口。你可以为每个客户在隧道端口上分配一个唯一的访问 VLAN ID，如图 4-5 所示。

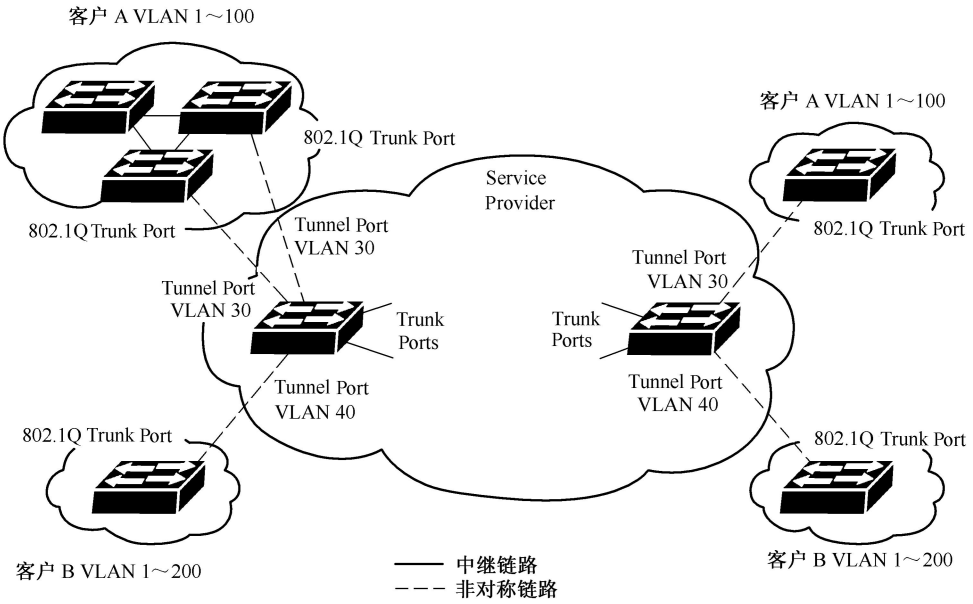

图 4-5　客户端 Trunk 端口与服务商 Tunnel 端口的连接示意图

从客户端中继端口进入到服务商边缘交换机隧道端口的数据包通常是以相应 VLAN ID 标记的 IEEE 802.1Q 包（在原来的以太网帧 Len/Etype 字段前插入了 Etype 和 Tag 两个字段）。这个标记包在离开客户端设备前是保持不变的，但进入到服务商网络时，它们将被另一层包含了分配给相应客户的 VLAN ID 的 IEEE 802.1Q 标记（称为 Metro Tag）进行封装（再在 Etype 字段前面插入 Etype 和 Tag 两个字段）。原来客户的 IEEE 802.1Q 标记仍被保留在封装包中，图 4-6 显示了双重标记数据包的结构。所以，数据包进入到服务商网络时，是包含了分配给客户的 VLAN ID 标记和流入通信的内部 VLAN ID 标记的双重标记。当双重标记的数据包进入服务商核心交换机上的一个中继端

口时，外层标记（Metro Tag）在数据交换时被剥离。当数据包从核心交换机上的另一个中继端口离开时，则又重新封装了 Metro Tag。

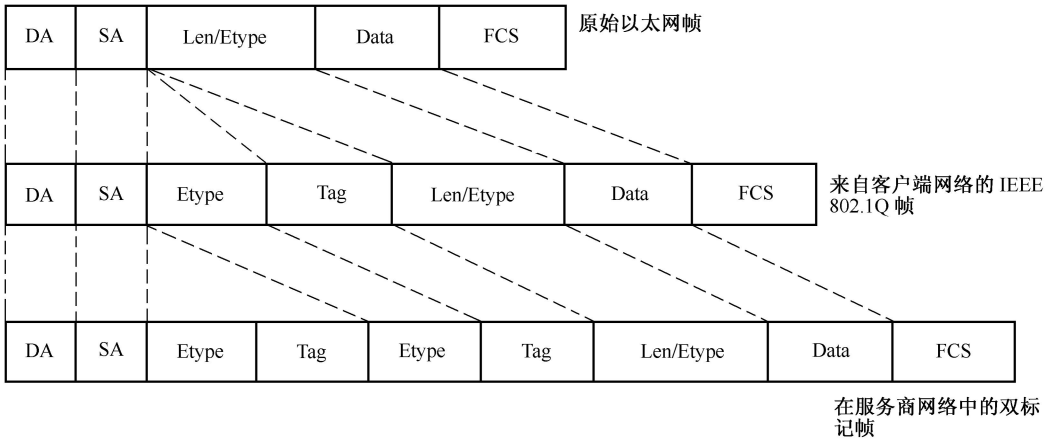

图 4-6　原始以太网帧、IEEE 802.1Q 帧和双标记以太网帧格式

当数据包进入到服务商出口交换机的中继端口时，外层标记又重新被剥离。此时数据包被直接发送到客户端的边缘交换机隧道端口，外层标记也不再封装在这个数据包上。数据包作为一个普通 IEEE 802.1Q 标记帧发送，保留客户端网络中自己的 VLAN ID 标记。

在图 4-5 中，服务商为客户 A 分配了一个 VLAN 30，而为客户 B 分配了一个 VLAN 40。进入客户边缘设备中继端口的包是带有 IEEE 802.1Q 标记的，进入到服务商网络时，将使用 VLAN ID 30 或 40 再次对这个数据包进行标记。而内层中标记的是他们各自内部的 VLAN ID，如 VLAN 100。即使在客户 A 和客户 B 的网络中都有 VLAN 100，他们在服务商网络中的通信仍是独立的，因为他们发送的数据包中，进入到服务商网络后被封装的外层标记是不一样的。每个客户可以控制他自己内部网络的 VLAN 空间，与其他客户和服务商网络所使用的 VLAN 空间都无关。在流出的隧道端口上，包中原来的客户端网络 VLAN ID 将被覆盖。

如果来自客户网络的通信是没有标记的（也就是为本地 VLAN 帧），这些数据包将被作为普通包进行桥接或被路由。所有通过服务商边缘设备隧道端口进入到服务商网络的包都将作为未标记包来处理，不管是否用 IEEE 802.1Q 头进行了标记。在数据包通过服务商网络 IEEE 802.1Q 中继端口发送时将用 Metro Tag VLAN ID 进行封装。在 Metro Tag 中的优先级（Priority）字段设置为隧道接口上配置的接口 CoS（Class of Service，服务分类）。如果没有配置 CoS，则优先级字段设为 0。

在 Catalyst 3750 系列交换机上，802.1Q 隧道是基于每端口来配置的，与交换机是独立交换机还是堆叠成员无关。如果是交换机堆叠，则所有配置均在堆叠主交换机上进行操作。

4.6.2　IEEE 802.1Q Tunneling 配置指南

默认情况下是禁止 IEEE 802.1Q 隧道协议的，因为默认的交换端口是动态自动模式（dynamic auto）。在所有 IEEE 802.1Q 中继端口上，用 IEEE 802.1Q 标记的本地 VLAN（Native VLAN）包是禁止的。

当配置 IEEE 802.1Q 隧道时，应当在客户端设备和服务商边缘交换机之间总是使用非对称链路，把客户端设备的流出端口配置为 IEEE 802.1Q 中继端口，服务商边缘交换机的流入端口配置为隧道端口。仅当 VLAN 使用隧道技术时才分配隧道端口。

当在服务商边缘交换机上配置 IEEE 802.1Q 隧道时，必须使用 IEEE 802.1Q 中继端口来发送数据包进入到服务商网络。但是无论如何，数据包通过服务商网络核心时可能要通过 IEEE 802.1Q 中

继、ISL 中继或者非中继链路。当在核心交换机上使用 IEEE 802.1Q 中继时，IEEE 802.1Q 中继的本地 VLAN（Native VLAN）不能与同一交换机上的任何非中继（隧道）端口的本地 VLAN 一样，因为在本地 VLAN 中的通信在 IEEE 802.1Q 中继端口上发送时是不进行标记的。

例如在图 4-7 中，假设服务商为客户 X 分配了一个 VLAN 40，而客户 X 在 Switch A 的中继端口上配置了本地 VLAN 40。现客户 X 的 Switch A 发送一个标记为 VLAN 30 的数据包到服务商网络 Switch B 中属于 VLAN 40 的隧道端口上。因为隧道端口的访问 VLAN 与客户 X 边缘交换机中继端口的本地 VLAN 一样，则 Metro 标记不会添加到从隧道端口上接收到的已标记数据包中，也就是不会再对该数据包封装服务商为客户 X 分配的 VLAN 40 标记。这样这个数据包就仅带有 VLAN 30 标记，通过 Switch B 和 Switch C 之间的中继链路直接转发，到达出口交换机 Switch C 的中继端口后会错误地从服务商边缘交换机隧道端口到达客户 Y 的 Switch E 交换机中继端口（本应是到达客户 X 的 Switch D 交换机中继端口），因为客户 Y 所连接的隧道端口正好属于 VLAN 30。

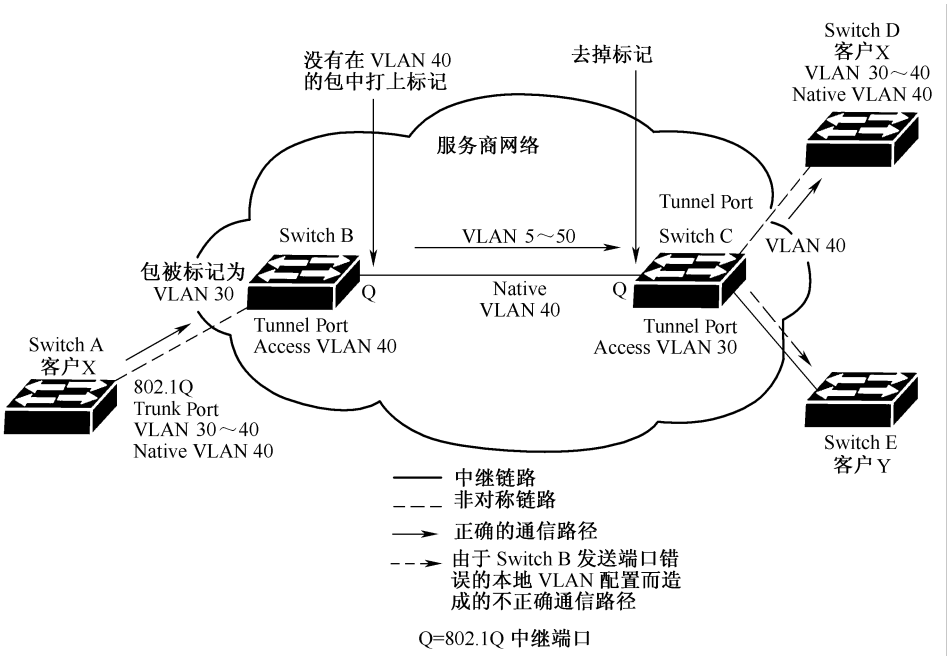

图 4-7　IEEE 802.1Q 隧道技术与本地 VLAN 同时使用时存在潜在的问题

为了解决这个问题，可以采取以下几种方法：

- 在服务商网络核心交换机间使用 ISL 中继方式。因为服务商网络客户端接口与客户端网络边缘交换机之间的连接必须是 IEEE 802.1Q 中继模式，所以建议在服务商核心交换机间使用 ISL 中继模式。
- 使用 **vlan dot1q tag native** 全局配置命令配置边缘交换机，以便所有流出 IEEE 802.1Q 中继端口的包（包括本地 VLAN）都将被标记。如果在所有 IEEE 802.1Q 中继端口上配置标记本地 VLAN 包，则交换机可以接收未标记包，但仅发送标记包。
- 确保在客户端网络边缘交换机中继端口上的本地 VLAN ID 不在客户 VLAN 范围之内。例如，如果中继端口承载的是 VLAN 100～200 的通信，则分配给客户的 VLAN ID 不要在这个范围内。

另外，尽管 IEEE 802.1Q 隧道可以很好地进行二层数据包交换，但仍有一些二层功能和三层交换在隧道端口上不兼容。具体如下：

- 隧道端口不能成为可路由端口。

- 在包括 IEEE 802.1Q 隧道端口的 VLAN 中不支持 IP 路由，在隧道端口上接收到的数据包仅进行二层转发。如果在一个包括隧道端口的 VLAN 的 SVI 上启用了 IP 路由，在隧道端口上接收到的非标记 IP 数据包可以被识别并被交换机路由。客户可以通过它的本地 VLAN 访问 Internet。如果这种访问不需要，则不要在包括隧道端口的 VLAN 上配置 SVI。
- 隧道端口不支持 Fallback Bridging，因为所有从隧道端口中接收到的 IEEE 802.1Q 标记数据包被看做是非 IP 数据包。如果在包含隧道端口的 VLAN 中启用 Fallback Bridging，IP 包将会通过 VLAN 不正确地桥接。所以，一定不要在包含隧道端口的 VLAN 中启用 Fallback Bridging。
- 隧道端口不支持 IP ACL。
- 隧道端口不支持三层 QoS ACL 和其他与三层信息相关的 QoS 功能，但支持基于 MAC 的 QoS。
- 只要在隧道端口上的 IEEE 802.1Q 配置与以太网通道组的配置一致，则以太网通道组与隧道端口可以兼容。
- 在 IEEE 802.1Q 隧道端口上支持 PAgP（Port Aggregation Protocol，端口聚合协议）、LACP（Link Aggregation Control Protocol，链路聚合控制协议）和 UDLD（UniDirectional Link Detection，单向链路检测）。
- DTP 不能与 IEEE 802.1Q 隧道兼容，因此必须手动配置非对称链路两端的隧道端口和中继端口。
- 在隧道中的非对称链路中不能运行 VTP。
- IEEE 802.1Q 隧道端口支持环路检测功能。
- 当一个端口被配置成 IEEE 802.1Q 隧道端口时，STP BPDU 过滤功能就会自动在接口上启用，而 CDP 和 LLDP 自动在接口禁用。

4.6.3 IEEE 802.1Q Tunnel 端口配置

可自特权模式开始，按照表 4-26 所示的步骤配置 IEEE 802.1Q 隧道端口。

表 4-26 IEEE 802.1Q 隧道端口的配置步骤

步骤	命令	说明
1	Switch#**configure terminal**	进入全局配置模式
2	Switch(config)#**interface** *interface-id*	键入要配置为隧道端口的二层接口并进入接口配置模式。这应该是服务商网络连接客户交换机的边缘端口。可以是物理接口或端口通道逻辑接口（端口通道号为 1～48）
3	Switch(config-if)#**switchport access vlan** *vlan-id*	为接口指定默认的 VLAN。这个 VLAN ID 是服务商分配给客户的
4	Switch(config-if)#**switchport mode dot1q-tunnel**	设置接口为 IEEE 802.1Q 隧道端口。可以使用 **no switchport mode dot1q-tunnel** 接口配置模式命令把端口设置恢复为默认的动态自适应（dynamic desirable）状态
5	Switch(config-if)#**exit**	返回全局配置模式
6	Switch(config)#**vlan dot1q tag native**	（可选）设置交换机在所有 IEEE 802.1Q 中继端口上启用本地 VLAN 数据包标记。如果不设置，客户的 VLAN ID 与本地 VLAN ID 一样，中继端口不会应用 Metro 标记，数据包将被发送到错误的目的地。 可以使用 **no vlan dot1q tag native** 全局配置模式命令禁止对本地 VLAN 数据包进行标记
7	Switch(config)#**end**	返回特权模式
8	Switch#**show running-config** Switch#**show dot1q-tunnel**	显示端口的 IEEE 802.1Q 隧道配置 显示处于隧道模式的端口
9	Switch#**show vlan dot1q tag native**	显示 IEEE 802.1Q 本地 VLAN 标记状态
10	Switch#**copy running-config startup-config**	（可选）保存以上配置更改到启动配置文件中

以下示例是先配置堆叠成员 1 交换机上的 gigabitethernet1/0/7 接口作为隧道端口，为客户分配的 VLAN ID 为 22，并启用本地 VLAN 数据包标记功能，然后校验所做的配置。

```
Switch(config)#interface gigabitethernet1/0/7
Switch(config-if)#switchport access vlan 22
% Access VLAN does not exist. Creating vlan 22
Switch(config-if)#switchport mode dot1q-tunnel
Switch(config-if)#exit
Switch(config)#vlan dot1q tag native
Switch(config)#end
Switch#show dot1q-tunnel interface gigabitethernet1/0/7
Port
-----
Gi1/0/1Port
-----
Switch#show vlan dot1q tag native
dot1q native vlan tagging is enabled
```