[1.交换机概述 2](#_Toc464331531)

[2.交换机的工作原理 2](#_Toc464331532)

[2.1第二层交换技术 3](#_Toc464331533)

[2.1.1 地址学习 3](#_Toc464331534)

[2.1.2 转发和过滤数据包 4](#_Toc464331535)

[2.1.3 消除回路 5](#_Toc464331536)

[2.2三层交换 5](#_Toc464331537)

[3.交换机内部结构 6](#_Toc464331538)

[3.1构造及主要功能 6](#_Toc464331539)

[3.2内部结构 7](#_Toc464331540)

[4. 交换机的工作机制 8](#_Toc464331541)

[4.1 交换机的工作原理 8](#_Toc464331542)

[4.1.1 构造及主要功能 8](#_Toc464331543)

[4.1.2 二层交换机的工作原理 8](#_Toc464331544)

[4.1.3 三层交换机的工作原理 9](#_Toc464331545)

[4.2 交换机的常规配置 10](#_Toc464331546)

[4.2.1 切换命令行界面模式 10](#_Toc464331547)

[4.2.2 基本交换机配置 10](#_Toc464331548)

[4.2.3 验证交换机配置 12](#_Toc464331549)

[4.2.4 基本交换机管理 13](#_Toc464331550)

# 1.交换机概述

交换机是一种基于MAC（网卡的硬件地址）识别，能完成封装转发数据包功能的网络设备，交换机正如它的名字一样采用的是交换的工作模式，它可以“学习”网络中各个终端的MAC 地址，并把其存放在内部的MAC 地址表中，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源地址到达目的地址。

交换机拥有一条很高很快的背部总线和内部交换矩阵。交换机的所有端口均挂接在这条背部总线上，当控制电路接收到数据包后，处理端口会查找内存中的MAC 地址对照表以确定目的MAC 地址的网卡接在哪个端口上，通过内部交换矩阵直接将数据包传送到目的端口，而不是所有端口，交换机的这种工作方式较于集线器来说效率高，不浪费网络资源，因为它只是对目的地址传输数据，发送数据是其他节点很难侦听到所发送的信息。这也是交换机能很快取代集线器的重要原因之一。

交换机的另一个重要特点是它不像集线器一样每个端口共享带宽，它的每一个端口都是共享一部分交换机的总带宽，这样在速率上就对每个端口有个根本的保障。这样交换机就可以在同一时刻进行多个端口之间数据传输，每个端口都视为独立的网段，享有独立固定的带宽。无需同其他设备竞争使用。

交换机的目的是使得传输效率更高，它根据MAC 地址来进行判断，决定数据帧该送到目的地址的连接端口，而不打扰其他不相干的连接端口，如果内存中的地址表中不包含目的MAC 地址，交换机则会向所有端口广播这个数据包，找到后再将这个MAC地址加入到自己的MAC 地址表中，这样下次发送到这个地址时便不会发错。

# 2.交换机的工作原理

交换机的主要工作原理有以下几条：

- 地址表：端口地址表记录了端口下包含主机的MAC地址。端口地址表是交换机上电后自动建立的，保存在RAM中，并且自动维护。交换机隔离冲突域的原理是根据其端口地址表和转发决策决定的。

转发决策：交换机的转发决策有三种操作：丢弃、转发和扩散。丢弃：当本端口下的主机访问已知本端口下的主机时丢弃。转发：当某端口下的主机访问已知某端口下的主机时转发。扩散：当某端口下的主机访问未知端口下的主机时要扩散。每个操作都要记录下发包端的MAC地址，以备其它主机的访问。

- 生存期：生存期是端口地址列表中表项的寿命。每个表项在建立后开始进行倒记时，每次发送数据都要刷新记时。对于长期不发送数据主机，其MAC地址的表项在生存期结束时删除。所以端口地址表记录的总是最活动的主机的MAC地址。

- 三层路由：通常，普通的交换机只工作在数据链路层上，路由器则工作在网络层。而功能强大的三层交换机可同时工作在数据链路层和网络层，并根据 MAC地址或IP地址转发数据包。但是要注意到三层交换机并不能完全取代路由器，因为它主要是为了实现处于两个不同子网的Vlan进行通讯，而不是用来作数据传输的复杂路径选择。

- 网管功能：一台交换机所支持的管理程度反映了该设备的可管理性与可操作性。带网管功能的交换机可对每个端口的流量进行监测，设置每个端口的速率，关闭/打开端口连接。通过对交换机端口进行监测，便于对网络业务流量的区分和迅速进行网络故障定义，提高了网络的可管理性。

- 端口聚合：这是一种封装技术，它是一条点到点的链路，链路的两端可以都是交换机，也可以是交换机和路由器，还可以是主机和交换机或路由器。基于端口汇聚（Trunk）功能，允许交换机与交换机、交换机与路由器、主机与交换机或路由器之间通过两个或多个端口并行连接同时传输以提供更高带宽、更大吞吐量， 大幅度提供整个网络能力。

## 2.1第二层交换技术

### 2.1.1 地址学习

以太网交换机通过学习地址来进行数据的转发操作。交换机开机启动后，会自动生成一张表，即MAC地址表，交换机关机后，MAC地址表中的内容会自动清空。

交换机MAC地址表用于记录连到交换机的所有设备的位置。交换机的目标是分割网上通信量，使发送到给定冲突域中主机的数据包不至于传播到另一个网段。这是由交换机的“学习”功能完成的，“学习”功能使交换机了解到主机位于哪里。交换机的学习和转发过程如下：

- 当一个交换机首次初始化时，交换机地址表是空的。

- 用一个空MAC地址表，基于地址的源过滤或转发决策是不可能的，因此交换机将每一帧转发给所有连接的端口，而不只是接受的端口。

- 转发一个帧到所有连接端口，称为“泛洪”。泛洪是一种通过交换机传输数据的低效方法，因为它将数据帧传输到了不需要的网段，浪费了带宽。

- 因为交换机能同时处理多个网段的通信量，交换机执行内存缓冲以致能独立接受、传输每个端口或网段的数据帧。

MAC地址表中的内容主要包括交换机端口、与交换机端口相连的主机MAC地址、VLAN标识。图3.1显示了不同网段间两个工作站之间的事务。MAC地址为0260.8c01.1111的站点A准备发送数据到MAC地址为0260.8c01.2222的站点C，交换机接受该帧，执行以下几个动作：

1. 从物理以太网接收该帧并且存储到临时缓冲区。

2. 因为交换机不知道哪个接口连到目的站点，它将帧泛洪给所有端口。

3. 当站点A泛洪该帧时，交换机在MAC地址表中记录发送数据包站点的源地址及与之相连的端口F0/1。

4. 如果该记录在一定时间内没有新的帧传到交换机来刷新，这个记录被废弃。

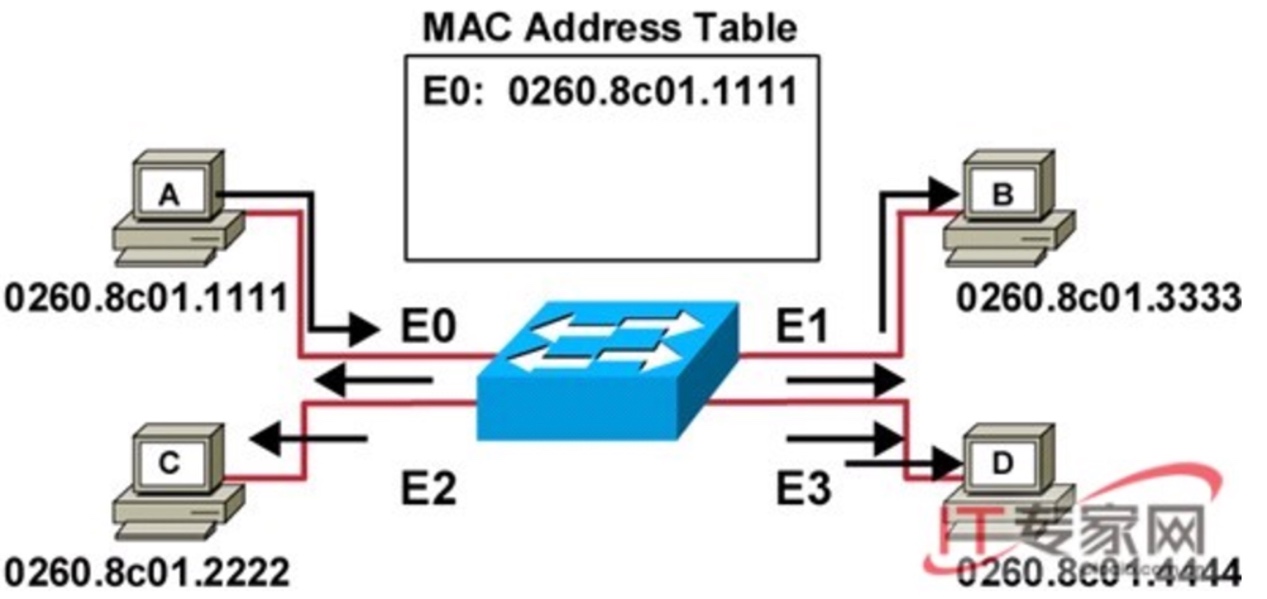


图2.1 泛洪数据包

当站点继续发送帧到另一个站点时，学习过程继续。MAC地址为0260.8c01.4444的站点D给MAC地址为0260.8c01.2222的站点C发送数据包，交换机采取以下几个动作：

1. 源地址0260.8c01.4444被加到MAC地址表中。

2. 将传输帧的目的MAC地址站点C与MAC地址表记录进行比较。

3. 当软件决定对这个目的地来说至此未见端口到MAC地址映射时，该帧被泛洪到交换机中所有的端口。

当站点A发送一帧到站点C时，交换机查询到站点C的MAC地址和端口F0/2，这里交换机将站点A发送的数据包直接转发给站点C，而不发送给B和D站点，如图3.2所示。只要在MAC地址表中记录生命周期内所有站点发送数据帧，就可以建立起完整的MAC地址表。

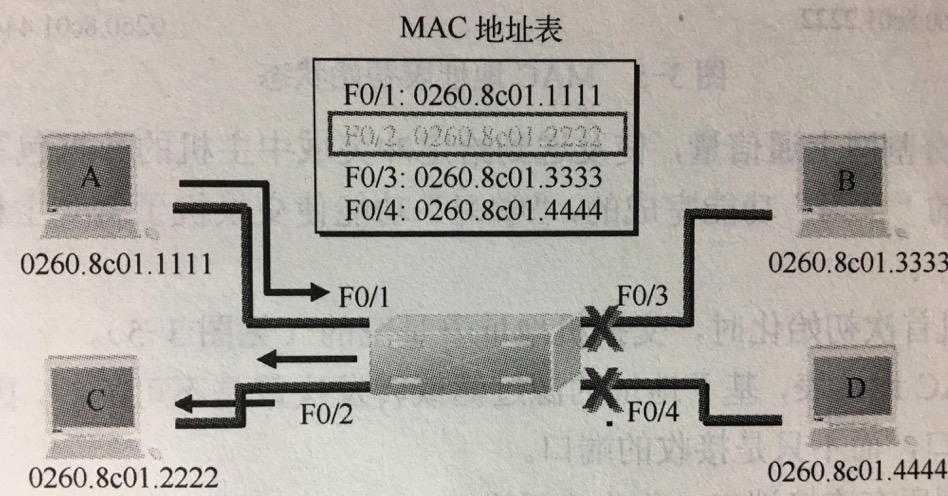


图3.2 站点应答

### 2.1.2 转发和过滤数据包

当一个帧带有一个已知目的地址到达时，它被转发到连接该站点而不是所有站点的端口。在图3.3中，站点A给站点C发送一帧。当目的MAC地址（站点C的MAC地址）已在MAC地址表中时，交换机只将帧传输到表中所列的这个端口。

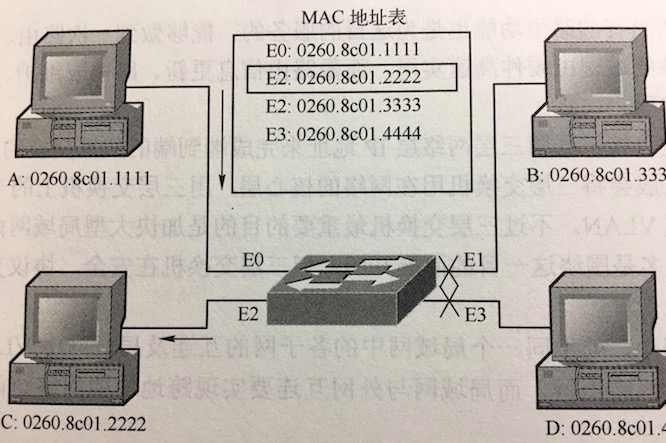


图3.3 交换机过滤决策

站点A发送帧给站点C的步骤如下：

1. 传输帧的目的MAC地址0260.8c01.2222与MAC地址表中项进行比较。

2. 当交换机决定目的地址经由E2端口可到达时，它将该帧传到该端口。

3. 交换机为了保护链路上的带宽没有将帧传到E1和E3口，这个动作称为“帧过滤”。

广播和组播是一个特殊情况。因为广播帧和组播帧可能所有站点都关心，交换机通常将广播帧和组播帧泛洪给出了发起端口外的所有端口。交换机从来不学习广播或组播地址，因为广播地址和组播地址不出现在帧的源地址中。所有站点接受广播帧的事实意味着所有交换网络中网段是在同一广播域中。

### 2.1.3 消除回路

交换机第三个功能是消除回路。桥接网路，包括交换网络，通常设计有荣誉链路和设备。这样的设计消除了一种可能性：一个节点的失败将导致整个交换网络的功能丢失。尽管冗余设计可能消除了单点失败问题，但也引入了几个值得考虑的问题：

- 如果没有回避规避服务，每个交换机就会无穷无尽地泛洪广播，这种情况通常称为网络回路（bridge loop）。这些广播通过回路不停地传播，产生了广播风暴，导致带宽浪费，严重影响网络和主机功能。

- 多份非广播帧传给目的站点。很多协议期望接受每个传输的单个副本，同一帧的多个副本可能导致不可恢复的错误。

- MAC地址表的不稳定导致同一帧的多副本在交换机的不同端口接收。当交换机在MAC地址表中因客服地址颠簸而消耗资源时，转发的数据可能被损坏。

## 2.2三层交换

三层交换技术，也称多层交换技术，是相对于传统交换概念而提出的。传统交换技术是在OSI模型的第二层——数据链路层进行操作的，而多层交换技术是在OSI模型的第三层实现了数据包的高速转发。简单地说，三层交换技术就是第二层交换技术+第三层转发技术，或者是将传统路由器的数据包处理功能和交换机的速度优势结合在一起的技术。三层交换机就是“二层交换机+基于硬件的路由器”。

三层交换机的路由记忆功能是由路由缓存来实现的。当一个数据包发往三层交换机时，三层交换机首先在它的缓存列表里进行检查，看路由缓存里是否有记录。如果有记录就直接调取缓存的记录进行路由，而不再经过路由处理器进行处理，从而大大提高了数据包的路由速度。如果没有发现记录，再将数据包发往路由处理器进行处理，处理之后再转发数据包。

两台处于不同子网的主机通信，必须通过路由器进行路由。在图3.4中，主机A向主机B发送的第1个数据包必须经过三层交换机中的路由处理器进行路由才能到达主机B，但是当以后的数据包再发向主机B时，就不必再经过路由处理器处理了，因为三层交换机有“记忆”路由的功能。

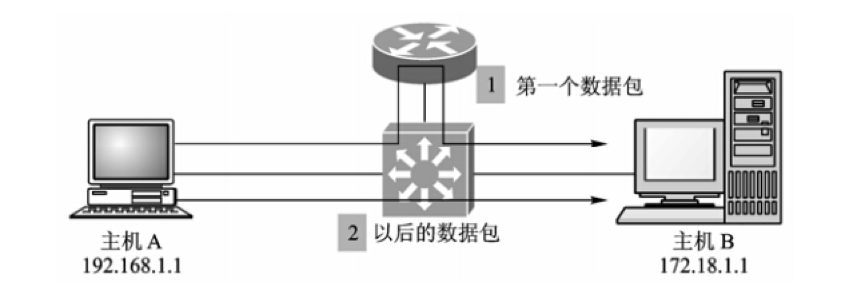


图3.4 三层交换技术原理

假设某主机A与主机B以前曾通过交换机进行通信，如果该交换机可以支持第三层交换，那么它便会将A和B的IP地址及它们的MAC地址记录下来。当其他主机C想要与A主机或者B主机进行通信时，在交换机接收到C所发出的寻址封包后，会立即送回给C一个回复信息包，并告诉它主机A或者主机B的MAC地址，那么以后主机C就会使用主机A或者B的MAC地址“直接”通信。因为通信双方并没有通过路由器进行“拆包”和“打包”的过程，所以即使主机A、B或者C分属于不同的子网，它们之间也可直接获取对方的MAC 地址来进行通信。

最重要的是，三层交换机并没有像其他交换机一样把广播封包扩散，三层交换机之所以叫三层交换机就是因为它可以获取第三层信息，如IP地址、ARP等。所以，三层交换机能知道某一广播封包的目的何在，在没有把它扩散出去的情形下，同时满足了发出该广播封包人的需求（不管它们在任何子网里）。因为三层交换机没有对数据包进行“拆包”和“打包”的工作，所有经过它的数据包不会被修改就传送到目的地。所以，应用三层交换技术即可实现网络路由的功能，又可以根据不同的网络状况做到最优的网络性能。

随着网络技术的不断发展，三层交换机有望在大规模网络中取代现有路由器的位置。

# 3.交换机内部结构

## 3.1构造及主要功能

交换机是一种基于MAC地址识别，能完成封装转发数据包功能的网络设备。交换机可以“学习”MAC地址，并把其存放在内部地址表中，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源地址到达目的地址。

传统的交换机工作在OSI 模型中的第二层，类似于一台专用的特殊计算机，主要包括中央处理器(CPU)、随机存储器(RAM)和操作系统。它利用专门设计的芯片ASIC(Application SpecificIntegratedCircuits)使交换机以线路速率在所有的端口并行进行转发，因此，它比同在二层利用软件进行转发的网桥速度快的多。

交换机拥有一条很高带宽的背部总线和内部交换矩阵。交换机的所有的端口都挂接在这条背部总线上，控制电路收到数据包以后，处理端口会查找内存中的地址对照表以确定目的MAC（网卡的硬件地址）的NIC（网卡）挂接在哪个端口上，通过内部交换矩阵迅速将数据包传送到目的端口，目的MAC若不存在才广播到所有的端口，接收端口回应后交换机会“学习”新的地址，并把它添加入内部MAC地址表中。

交换机使用一种虚拟连接技术来连接通信的双方。所谓虚拟连接，就是指通信时通信双方建立一个逻辑上的专用连接，这个连接直到数据传送至目的节点后结束。虚拟连接是通过交换机的端口-地址表来实现的：交换机在工作过程中不断地建立和维护它本身的一个地址表，这个地址表标明了节点的MAC地址和交换机端口的对应关系。当交换机收到一个数据包，它便会去查看自身的地址表以验明数据包中的目的MAC地址究竟对应于哪个端口。一旦验证完毕，就将发送节点与该端口建立一个专用连接，发送方的数据仅发送到目的MAC 地址所对应的交换机端口。

## 3.2内部结构[[1]](#footnote-1)

局域网交换机卓越的性能表现，来源于其内部独特的技术结构。而不同的交换模式或不同的交换类型，也跟局域网交换机内部结构密不可分。所以说，了解了局域网交换机的内部结构，就等于了解了局域网交换机的技术特点和工作原理。目前局域网交换机采用的内部技术结构主要有以下几种。

1. 共享内存式结构

该结构依赖于中心局域网交换机引擎所提供的全端口的高性能连接，并由核心引擎完成检查每个输入包来决定连接路由。这种方式需要很大的内存带宽和很高的管理费用，尤其是随着局域网交换机端口的增加，需要内存容量更大，速度也更快，中央内存的价格就变得很高，从而使得局域网交换机内存成为性能实现的主要瓶颈。

2. 交叉总线式结构

交叉总线式结构可在端口间建立直接的点对点连接，这种结构对于简单的单点式（Unicast）信息传输来讲性能很好，但并不适合点对多点的广播式传输。由于实际网络应用环境中，广播和多播传输方式很常见，所以这种标准的交叉总线方式会带来一些传输问题。例如，当端口A向端口D传输数据时，端口B和端口C就只能等待。而当端口A向所有端口广播消息时，就可能会引起目标端口的排队等候。这样将会消耗掉系统大量带宽，从而影响局域网交换机传输性能。而且要连接N个端口，就需要N×（N+1）条交叉总线，因而实现成本也会随着端口数量的增加而急剧上升。

3. 混合交叉总线式结构

鉴于标准交叉总线存在的缺陷，一种混合交叉总线实现方式被提了出来。该方式的设计思路是将一体的交叉总线矩阵划分成小的交叉矩阵，中间通过一条高性能总线连接。该结构的优点是减少了交叉总线数，降低了成本，还减少了总线争用。但连接交叉矩阵的总线成为新的性能瓶颈。

4. 环形总线式结构

这种结构方式在一个环内最多可支持四个交换引擎，并且允许不同速度的交换矩阵互连，以及环与环间通过交换引擎连接。由于采用环形结构，所以很容易聚集带宽。当端口数增加的时候，带宽就相应增加了。与前述几种结构不同的是，该结构方式有独立的一条控制总线，用于搜集总线状态、处理路由、流量控制和清理数据总线。另外，在环形总线上可以加入管理模块，提供完整的SNMP管理特性。同时还可以根据需要选用第三层交换功能。这种结构的最大优点就是扩展能力强，实现成本低，而且有效地避免了系统扩展时造成的总线瓶颈。

# 4. 交换机的工作机制

## 4.1 交换机的常规配置

以Cisco交换机为例，说明交换机的一些常规配置。

### 4.1.1 切换命令行界面模式

作为一项安全功能，Cisco IOS软件将EXEC（执行）会话分成以下两种访问级别。

用户执行：只允许用户访问有限量的基本监视命令。用户执行模式是在从CLI登录到Cisco交换机后所进入的默认模式。用户执行模式由">"提示符标识。

特权执行：允许用户访问所有设备命令，如用于配置和管理的命令，特权执行模式可采用口令加以保护，使得只有获得授权的用户才能访问设备。特权执行模式由#提示符标识。

要从用户执行模式切换到特权执行模式，输入enable命令。要从特权执行模式切换到用户执行模式，输入disable命令。在实际网络中，交换机将提示输入口令。默认情况下未配置口令。表1-1中显示了用于在用户执行模式和特权执行模式之间来回切换的Cisco IOS命令。

表4-1 执行模式切换

|  |  |
| --- | --- |
| 说    明 | CLI |
| 从用户执行模式切换到特权执行模式 | Switch>enable |
| 如果已为特权执行模式设置口令，则系统将提示您现在输入口令 | Password:password |
| #提示符表示已处于特权执行模式 | Switch# |
| 从特权执行模式切换到用户执行模式 | Switch#disable |
| >提示符表示已处于用户执行模式 | Switch> |

在Cisco交换机上进入特权执行模式之后，就可以访问其他配置模式。Cisco IOS软件的命令模式结构采用分层的命令结构。

### 4.1.2 基本交换机配置

局域网中的第2层交换机的一些关键配置序列通常是在实施过程中进行的。这些配置序列包括配置交换机管理界面，默认网关，全双工和活动接口上的网速设置，对HTTP访问的支持和对MAC地址表的管理。

1. 管理接口

接入层交换机需要配置IP地址、子网掩码和默认网关。要使用TCP/IP来远程管理交换机，就需要为交换机分配IP地址。此IP地址将分配给称为虚拟LAN（VLAN）的虚拟接口，然后必须确保VLAN分配到计算机上的一个或多个特定端口。

要在交换机的管理VLAN上配置IP地址和子网掩码，必须处在VLAN接口配置模式下。先使用命令interface vlan 99，再输入ip address配置命令。必须使用no shutdown接口配置命令来使此第3层接口正常工作。当看到"interface VLAN x"时，这是指与VLAN x 关联的第3层接口。只有管理VLAN才有与之关联的"interface VLAN"。表1-2列出了Catalyst 2960交换机上的管理接口配置。

表4-2 管理接口配置

|  |  |
| --- | --- |
| 说    明 | 命    令 |
| 进入全局配置模式 | S1#configure terminal |
| 进入VLAN99接口的接口配置模式 | S1(config)#interface vlan 99 |
| 配置接口IP地址 | S1(config-if)#ip address 172.17.99.11 255.255.255.0 |
| 启动接口 | S1(config-if)#no shutdown |
| 返回特权执行模式 | S1(config-if)#end |
| 进入全局配置模式 | S1#configure terminal |
| 输入要分配VLAN的接口 | S1(config)#interface fastethernet 0/18 |
| 定义端口的VLAN成员模式 | S1(config-if)#switchport mode access |
| 将端口分配给VLAN | S1(config-if)#switchport access vlan 99 |
| 返回特权执行模式 | S1(config-if)#end |
| 将运行配置保存为交换机启动配置 | S1#copy running-config startup-config |

1. 默认网关

默认网关是用于将IP数据包转发到远程网络的机制。交换机将目的IP地址位于本地网络之外的IP数据包转发到默认网关。

使用ip default-gateway命令，为交换机配置默认网关。输入与需要配置默认网关的交换机直接相连的下一跳路由器接口的IP地址。

1. 双工和速度

可以使用duplex接口配置命令指定交换机端口的双工操作模式。可以手动设置交换机端口的双工模式和速度，以避免厂商间的自动协商问题。在将交换机端口双工设置配置为auto时可能出现问题，在图1-1中，S1和S2交换机有着相同的双工设置和速度，这是例1-1中的配置产生的。

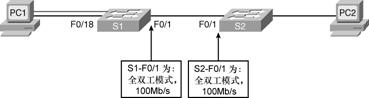


图4-1 双工和速度

在交换机S1上配置端口F0/1的具体步骤描述如例1-1所示。

S1# configure terminal

S1(config)# interface fastethernet 0/1

S1(config-if)# duplex auto

S1(config-if)# speed auto

S1(config-if)# end

例4-1 duplex和speed命令

1. HTTP访问

如例1-2是启用HTTP访问的基本配置，ip http authentication enable 是全局配置命令模式。

例4-2 启用HTTP访问的基本配置

S1# configure terminal

S1(config)# ip http authentication enable

S1(config)# ip http server

1. 管理MAC地址表

交换机使用MAC地址表来确定如何在端口间转发流量。这些MAC表包含动态地址和静态地址。用show mac-address-table命令显示MAC地址表，其输出包含静态和动态MAC地址。

使用mac-address-table static MAC-address vlan vlan-id interface interface-id命令可在MAC地址表中创建静态映射。使用no mac-address-table static MAC-address vlan vlan-id interface interface-id命令可移除MAC地址表中的静态映射。

### 4.1.3 验证交换机配置

执行初始交换机配置之后，可使用不同的show命令来验证交换机是否已正确配置。

show命令从特权执行模式下执行。表4-3列出了show命令的一些关键选项，它们可用于验证几乎所有可配置的交换机功能。

表4-3 show命令

|  |  |
| --- | --- |
| 说    明 | 命    令 |
| 显示交换机上单个或全部可用接口的接口状态和配置 | show interface {*interface-id*  ¦*cr*} |
| 显示启动配置的内容 | show startup-config |
| 显示当前运行配置 | show running-config |
| 显示关于flash：文件系统的信息 | show flash: |
| 显示系统硬件和软件状态 | show version |
| 显示会话命令历史记录 | show history |
| 显示IP信息 Interface选项显示IP接口状态和配置 http选项显示有关正在交换机上运行的Device Manager的HTTP信息 arp选项显示IP ARP表 | show ip {*interface | http*|*arp* } |
| 显示MAC转发表 | show mac-address-table |

### 4.1.4 基本交换机管理

交换机启动并运行之后，网络技术人员必须对交换机进行维护，这就包括备份和恢复交换机的配置文件，清除配置信息和删除配置文件。

1. 备份和恢复交换机配置文件

使用copy running-config startup-config特权执行命令备份了目前创建的配置。如果想在设备上保留多个不同的startup-config文件，则可以使用copy startup-config flash:filename命令将配置复制到不同文件名的多个文件中。存储多个startup-config版本可用于在配置出现问题时回滚到某个时间点。

恢复配置是一个简单的过程。只需用已存配置覆盖当前配置即可。例如，如果有名为config.bak1的已存配置，则输入Cisco IOS命令copy flash:config.bak1 startup-config即可覆盖现有start-config并恢复config.bak1的配置。当配置恢复到startup-config中后，可在特权执行模式下使用reload命令重新启动交换机，如表1-4所示，使计算机重新加载新的启动配置。reload命令将使系统停止。应在配置信息已输入到文件并保存到启动配置之后再使用reload命令。

表4-4恢复备份文件

|  |  |
| --- | --- |
| 说    明 | CLI |
| 将存储在闪存中的config.bak1文件复制到存储在闪存中的启动配置中。按Enter键接受，使用Ctrl+C组合键取消 | S1#copy flash:config.bak1 startup-config Destination filename [startup-config]? |
| 使Cisco IOS执行重新启动交换机。如果修改了运行配置文件，系统将询问是否保存。请按“y”或“n”确认。要确认重新装入，请按Enter键接受，使用Ctrl+C组合键取消 | S1#reload System configuration has been modified. Save?[yes/no]:n Proceed with reload?[confirm] |

1. 清除配置信息

交换机配置的清除使用erase nvram:或erase startup-config特权执行命令实现。当网络技术人员可能执行了一项很复杂的配置任务，并在闪存中存储了文件的很多备份副本，此时要从闪存中删除文件，要使用delete flash:filename特权执行命令。根据file prompt全局配置命令的设置，系统可能在技术人员删除文件之前提示确认。默认情况下，在删除文件时，交换机都会提示确认。抹除或删除配置之后，即可重新加载交换机以启动交换机的新配置。

1. 《网络安全实用技术标准教程》第87页，作者:李伟，清华大学出版社。 [↑](#footnote-ref-1)