第 1 章　交换机的结构与基本功能

知识要点：

交换机用做网络集中设备，其端口连接网络中的主机。在转发数据帧时，端口带宽能够独享。

交换机按其工作在 OSI 参考模型的对应层次，有第二层、第三层和第四层交换机。

可管理的交换机内置了操作系统软件。

第二层交换机采用帧交换转发数据，帧交换方式有三种，分别为存储转发、伺机通过和自由分段。

使用备份连接是提高网络可靠性的常用方法，但所形成的环路可能会导致广播风暴和引起多帧副本问题。

STP 协议的应用则可消除环路问题，使冗余备份得以实现。

1.1　交换机的作用与组成

在以太网络中，交换机起的是信息中转站的作用。它把从某个端口接收到的数据从其他端口转发出去。以下介绍交换机的外观与内部组成。不同厂家、不同型号的以太网交换机，其外观和内部组成都有一定的个性差异，但其共性是主要的。

1. 交换机的外观

前面板上的多个 RJ45 接口是以太网口，用来连接计算机或其他交换机。

后面板上的串口是交换机的配置口，用串口线缆将其与计算机的串口连接起来，可实现对交换机的配置操作。也有的交换机的配置口位于前面板上。

面板上有若干指示灯，其亮、灭或闪烁可以反映交换机的工作状态是否正常。

此外还有电源插口、电源开关等。

可上机架(柜)式交换机的标准长度为 48.26cm(19in)。

如图 1.1所示的是 Cisco Catalyst3550 和 Cisco Catalyst 2900 交换机的外观图。

2. 交换机的内部组成

交换机的内部组成为：

CPU （中央处理器）交换机使用特殊用途集成电路芯片 ASIC，以实现高速的数据传输。

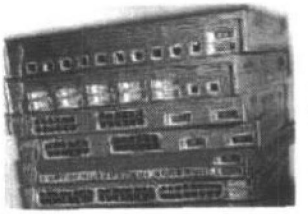
RAM/DRAM　主存储器，存储运行配置。

NVRAM(非易失性 RAM）存储备份配置文件等。

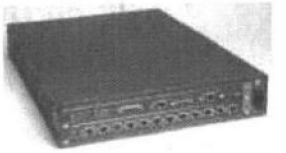
FlashROM （快闪存储器）存储系统软件映像，启动配置文件等。是可擦可编程的 ROM.

ROM　存储开机诊断程序、引导程序和操作系统软件。

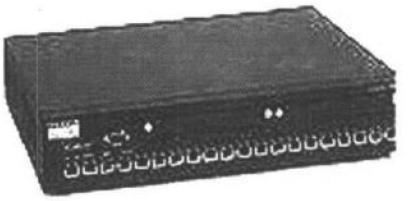
• 接口电路　交换机各端口的内部电路。



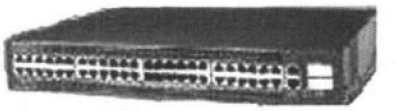
Catalyst 3550 系列



Catalyst 2900 系列



catlyst3700



catlyst2948

图 1.1　交换机的外观

1.2　交换机的分类

可按多种方式对交换机进行分类。若参照开放系统互连参考模型 OSI,则交换机属于第二～四层的设备。

1.2.1　OSI 参考模型与数据通信设备

开放系统互连参考模型 OSI 分为七层，每层的名称、对应的协议数据单元的名称以及每层所用的设备见表 1.1。

表 1.1　OSI 参考模型的层次及其相应设备

层数	名称	协议数据单元名称	相应设备
第七层	应用层	Data	
第六层	表示层	Data	
第五层	会话层	Data	
第四层	传输层	Segment	四层交换机
第三层	网络层	Paket	路由器、三层交换机
第二层	数据链路层	Frame	交换机、网桥
第一层	物理层	bit	网卡、网线等

根据 OSI 参考模型，每一层都使用相应的协议实现特定的功能，完成数据交换。高层数据逻辑地在源主机与目标主机对应层之间进行传输，屏蔽下层的细节。而数据实际的传输过

程则是：高层数据经过下面各层，依次被各层进行封装，最后通过物理层完成比特流的传输。

交换机可以工作在第二、第三、第四层，对应的技术称为第二层、第三层和第四层交换技术，第二层交换机是目前使用最多的交换机。

本书主要介绍第二层交换技术和第二层交换机。如无特别说明，以下提到的交换机均指第二层交换机。

1.2.2 交换机的简单分类

这里只对以太网交换机按配置是否可以改变或者按在 OSI 参考模型中的对应层次来进行简单的分类。

1. 模块式与固定配置式

按交换机的配置可否改变，可把交换机分为模块式和固定配置式。

- 模块式模块式交换机的模块可以拔插，模块通常是 100Mb/s 或 1 000Mb/s光纤接口模块,或 1 000Mb/s RJ45 接口模块，或者是堆叠模块。交换机上则有相应的插槽。使用时，模块插入插槽之中。模块式交换机配置灵活，模块可按需要购买。一般说来，模块式交换机的档次较高，模块插槽结构可最大程度地保护用户的投资。
- 固定配置式固定配置式交换机的接口固定，硬件不可升级。

2. 第二层、第三层与第四层交换机

前面已提过，按交换机工作在 OSI 参考模型的相应层次，交换机可分为三个层次的交换机，其中大量商品化的是第二层和第三层交换机。

- 第二层交换机第二层交换机工作在 OSI 参考模型的第二层，它的每个端口拥有自己的冲突域。如果该二层交换机具有虚拟局域网（VLAN)功能,则每一个 VLAN 成为一个广播域。第二层交换机采用三种方式转发数据帧：直通（Cut Through)、存储 -转发(Store-and-Forward)和自由分段(Fragment Free)。
- 第三层交换机第三层交换机根据目的 IP 地址转发数据报，与后面要讨论的路由器一样，它也必须创建和动态维护路由表。但是，第三层交换机能做到“一次路由，多次交换”。即是说，第三层交换机能够把报文转发到不同的子网，并在后续的通信中实现比路由更快的交换。
- 第四层交换机第四层交换机可以解释第四层的传输控制协议（TCP)和用户数据报协议(UDP)信息，允许设备为不同的应用（使用端口号区分）分配各自的优先级。这样,第四层交换机可以‘智能化”地处理网络中的数据,最大限度地避免拥塞,提高带宽利用率。

1.3 交换机在网络中的连接及作用

1.3.1 交换机的端口

以太网交换机的端口或称接口，是 8 个引脚的 RJ45 接口，其种类通常有 10Base-T，10Base-F、100Base-TX，100Base-T4 、100Base-FX，100Base-T、1000Base-FX 及 1000Base-T

等。

其中 Base 指的是采用基带传输技术，10、100 和 1 000 分别代表传输速率为 10Mb/s、100Mb/s 和 1 000Mb/s，通常把对应的技术分别称为以太网、快速以太网和千兆位以太网。

各参数的含义见表 1.2。

表 1.2 交换机的各种端口

标准类型		传输速率(Mb/s)	接口标准	传输介质	传输距离(m)	备注
10Base-T		10	RJ45	UTP(非屏蔽双绞线)	100	
10Base-F		10	光纤接口	62.5/125MMF(多模光纤)	2 000	
100Base-TX		100	RJ45	UTP	100	
100Base-T4		100	RJ45	UTP(4 对芯线)		
100Base-FX		100	光纤接口	62.5/125MMF	412	半双工
				62.5/125MMF	2 000	全双工
				9/125SMF(单模光纤)	10 000	
1000Base-CX		1 000	RJ45	STP(屏蔽双绞线)	25	
1000Base-T		1 000	RJ45	UTP(4 对芯线)	100	
1000Base-FX	-SX(780nm 短波)	1 000	光纤接口	62.5/125MMF	260	不同公司的产品实际支持的距离可能不同
				50/125MMF	525	
	-LX(1 300nm 长波)			62.5/125MMF	550	
				50/125MMF	550	
				9/125SMF	3 000 ~ 10 000	

1.3.2 共享式与交换式网络

采用双绞线或光纤作传输介质的网络，使用集线器或交换机作为网络的中心。计算机之间的通信，通过集线器或交换机进行数据的转发。

1. 集线器与共享式局域网

集线器通常称为 Hub，按其使用的技术可分为被动式与主动式集线器。前者只提供简单的集中网线转发数据的工作，后者可对数据作一定的处理。

集线器按端口的传输速率或俗称带宽来分，有 10Mb/s 和 100Mb/s 的。通常所说的集线器是指的共享式集线器，其带宽是所有端口共享的。例如一台 16 端口的 100Mb/s 的集线器，当全部端口都使用时，每一端口的带宽就只有 100Mb/s 的 1/16。由集线器作中心设备的局域网(以及总线型拓扑的局域网)称为共享式局域网。

集线器的全部端口属于同一个冲突域，集线器在端口之间转发数据帧时采用向所用端口广播的方式进行，因此其全部端口又属于同一个广播域。单一的冲突域和广播域使网络在通信繁忙时容易产生阻塞和广播风暴。

可以使用多台集线器级联或堆叠起来以增加总的端口数，但不能用此方法来延伸网络的

距离。

随着交换机价位的降低，共享式集线器正逐渐淡出局域网领域。

2. 交换机与交换式局域网

交换机可以看做是高档的集线器，它有时也被称之为交换式集线器。它采用了许多新的技术，如其端口之间的通信可全双工进行，能实现数据的线速转发等。它的最显著的特点在于端口带宽的独享。

例如一台 100Mb/s 的交换机，在使用时每一对端口之间的数据传输速率都是 100Mb/s，不会随着使用的端口数的增加而减少。即是说，其端口带宽是独享的。

应当注意的是，只有网卡和交换机两者的带宽都为同一值时，才能实现以该速率传输数据。否则，只能按二者中较小的一个速率传输。例如，只有网卡和交换机都是 1 000Mb/s 的，才能实现 1 000Mb/s 的传输速率。而且，使用的传输介质还必须支持该传输速率。这一特性称为带宽的自动协商或者带宽的自适应。

光纤能支持 1 000Mb/s 以上的传输速率，但使用光纤的网络未必都是千兆位以太网，最初的光纤以太网就是 10Mb/s 的。

通常把由交换机作为中心设备的局域网称为交换式局域网。

交换机的端口按其带宽可分为 10Mb/s，100Mb/s，10/100Mb/s 自适应和 1 000Mb/s 的，有的交换机上只有上列端口之一；更多的则是兼有两种或多种端口。

交换机的每一个端口都是一个冲突域，故不会因端口的使用数增加而降低端口的传输带宽。不过，交换机的所有端口仍属于同一个广播域，当网络中的广播信息增多时，也会导致网络传输效率的降低。

如果采用虚拟局域网(Virtual Local Network，VLAN)技术，则每一个 VLAN 具有各自的广播域，这样交换机就有了多个广播域。广播数据帧被局限在各自的域内，可有效防止广播风暴的发生。

与集线器一样，也可使用多台交换机级联或堆叠起来增加总的端口数。然而，交换机的级联却可以用来延伸网络的距离，如图 1.2 所示的级联可使网络范围扩展 400m。

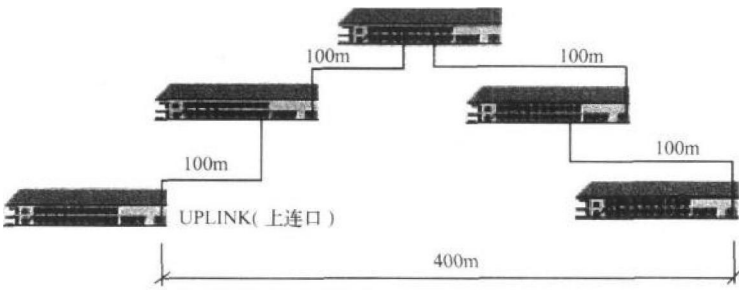


图 1.2 级联交换机以扩展网络距离

最廉价的交换机可能不支持网络管理功能，用于简单的网络环境。支持网络管理功能的交换机称为可管理或可配置的交换机。

若用在小型、简单的网络中，可管理的交换机也不需配置(实际是使用了默认配置)即可工作；而网络规模较大或者较为复杂时，就需要对其进行配置和管理了。

1.4 交换技术基础

连接在交换机端口上的主机通过地址解析协议 ARP 相互查询对方网卡的物理地址（又称 MAC 地址，即 Media Access Control 地址），以便进行相互间的数据帧的传输。

MAC 地址是固化在网卡内部用于惟一确定网卡身份的标识，是网卡在生产时被永久写入芯片的固定值。全球的网卡生产厂商按照买得的 MAC 地址范围制造网卡，因此不会有两块相同 MAC 地址的网卡。这样，MAC 地址就可用做惟一标识设备的地址。第二层交换过程通过使用 MAC 地址在低层实现通信寻的，即是说，网络中的数据包最终是通过 MAC 地址找到目标的。

由于交换机在数据传递过程中不用检查第三层（网络层）的包头信息，而是直接由第二层帧结构中的 MAC 地址来决定数据的转发目标，因此，数据的交换过程几乎没有软件的参与，从而大大提高了交换进程的速率。

1.4.1 MAC 地址数据库的建立与路由过滤

在交换式网络中，各主机的 MAC 地址是存储在交换机的 MAC 地址表（也称 MAC 地址数据库）中的。交换机在工作过程中，会向 MAC 地址表不断写入新学到的 MAC 地址。一旦交换机掉电或重新上电后，其内部的 MAC 地址表会被自动清空或清空后又重新建立。

1. MAC 地址表的建立

如图 1.3 所示，MAC 地址表的建立过程如下：

a. 工作站 1 向目标主机（工作站 3）发送查询（目标 MAC）地址信息，此时，该信息会首先发送到本地交换机 Switch。

b. 本地交换机在收到查询信息后，会先将信息帧内的源 MAC 地址记录在自己的 MAC 地址表中。然后，交换机再向其他所有端口发送查询信息。

c. 目标主机接收到该信息后，会通过交换机直接对源地址主机进行响应。此时，交换机就将工作站 3 的 MAC 地址也记录在其 MAC 地址表里。

d. 两台主机（工作站 1 和工作站 3）进行点对点的连接通信。

e. 如果两台主机在一定时间内未进行通信，交换机将会定时刷新数据库里的地址记录。

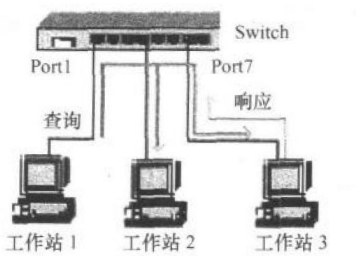


图 1.3 MAC 地址表的建立

2. MAC 地址表的路由过滤

当交换机接收到一个数据帧时，它会首先检查数据帧里的 MAC 地址，如果该地址未缓存

在 MAC 地址表里，交换机就向所有的其他端口发送查询信息；如果该地址已缓存在 MAC 地址表里，它就会按照表中的地址进行转发，而不会广播到其他端口，这样就可以减少对资源的占用，显著提高信息的交换速率。

以上称为交换机的 MAC 地址表的缓存过滤或路由过滤功能。

1.4.2 局域网的三种帧交换方式

局域网交换机在传送数据时，采用帧交换(Frame Switching)，该技术包括三种主要的交换方式，即存储转发(Store and Forward)、伺机通过(Cut Through)和自由分段(Fragment Free)。

1. 存储转发

存储转发(Store and Forward)方式是最基本的交换技术之一在进行转发数据帧前，该数据帧将被完全接收并存储在缓冲器中，数据帧从头到尾全部接收完毕才进行转发。其间，交换机需要解读数据帧的目的地址与源地址，并在 MAC 地址列表中进行适当的过滤。

在存储转发过程中还要进行高级别的冗余错误检测(CRC)工作，如果所接收到的数据帧存在错误、太短(小于 64B)或太长(大于 1 518B)，最终都会被抛弃。

采用这种转发方式的交换机在接收数据帧时延迟较大，且越大的数据帧延迟时间越长。

2. 伺机通过

伺机通过(Cut Through)技术是交换机在接收整个数据帧之前读取数据帧的目的地址到缓冲器，随后再在 MAC 地址列表里进行适当的过滤。

采用这种转发方式，在整个数据帧完全接收之前就已经转发了。这种方法减少了传输的延迟，但同时也削减了对数据帧的错误检测能力。

还有些交换机可以把存储转发与伺机通过两种技术合并在一起使用。它们首先在交换机里设置一个错误检测的门限值，当错误发生率低于该值时使用伺机通过的交换方法以减少数据的传输延迟，当误码率提高大于该门限值时，交换机将自动改为存储转发交换方式，从而保证了数据的正确性与准确性。在链路恢复正常后，误码率下降低于该门限值后，系统将再次回到伺机通过方式工作。

3. 自由分段

自由分段(Fragment Free)技术是在伺机通过交换方式的基础上调整的。自由分段在转发数据之前，过滤有包错误的冲突分段(长度为 64B)这是因为通常认为数据帧的错误总是发生在刚开始的 64B 内，自由分段交换方式的错误检测级别要高于伺机通过交换方式。

1.4.3 冗余备份与环路

在许多交换机或网桥设备组成的网络环境中，通常都使用一些备份连接，以提高网络的健壮性、稳定性。备份连接也称备份链路、冗余链路等。备份连接如图 1.4 所示，交换机 Switch1 的端口 Port7 与交换机 Switch3 的端口 Port6 之间的链路就是一个备份连接。在主链路（图中 Port1 与 Port3 之间的链路）出故障时，备份链路自动启用，从而提高网络的整体可靠性。

使用冗余备份能够为网络带来许多好处，但是备份连接使网络存在环路。图 1.4 中 Port1 - Port5 - Port8 - Port3 - Port6 - Port7 - Port1 就是一个环路。环路问题是备份连接所面临的

所有负面影响中最为严重的问题，它直接导致以下麻烦：

- 广播风暴
- 多个广播帧副本

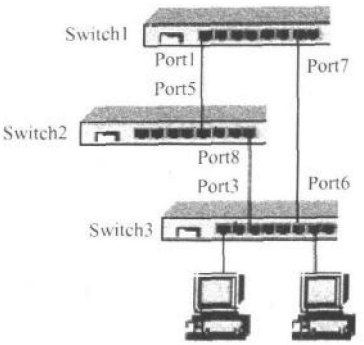


图 1.4　备份连接与环路

1. 广播风暴

在一些较大型的网络中，当大量广播流(如 MAC 地址查询信息等）同时在网络中传播时，便会发生数据包的碰撞。随后，网络试图缓解这些碰撞并重传更多的数据包，结果导致全网的可用带宽阻塞，并最终使得网络失去连接而瘫痪。这一过程被称为广播风暴。

网络中，一台设备能够将数据包转发给网络中所有其他站点的技术称为广播。由于广播能够穿越由普通网桥或交换机连接的多个局域网段，因此几乎所有局域网的网络协议都优先使用广播方式来进行管理与操作。广播使用广播帧来发送、传递信息，广播帧没有明确的目的地址，它所发送的对象是网络中的所有主机，也就是说网络中的所有主机都将接收到该数据帧。它一般用来广播网络中的公共信息，例如服务通告、地址查询等信息。

应用程序与协议的广播是引起广播风暴的主要原因。但是，在正常的网络环境中，网络广播是无所不在的。MAC 地址查询、路由协议通信、ICMP 控制报文以及大量的服务通告等信息都属于网络中正常的广播。因此需要在保证网络正常使用广播的情况下，有效减少广播风暴的发生。

广播风暴的形成：

在如图 1.4 所示的网络中，本来的打算是要提供冗余备份：Switch3 通过 Port6 与 Switch1 的 Port7 连接起来，增加一条 Switch3 到 Switch1 的通路。但结果却不能正常工作，这是一个存在循环的连接。

如果 Switch1 收到一个广播帧，下面的过程 a ~ f 会被反复执行：

a. Switch1　向 Port1 转发广播帧。

b. Switch2 通过 Port5 收到广播帧。

c. Switch2　向 Port8 转发广播帧。

d. Switch3 通过 Port3 收到广播帧。

e. Switch3　向 Port6 转发广播帧。

f. Switch1 通过 Port7 再次收到原来的广播帧，又从 a 开始重复以上过程。上述过程周而复始，同样的广播帧被不断复制，最后形成广播风暴，耗尽网络资源。

在一个较大规模的网络中，由于拓扑结构的复杂性，会造成许多大大小小的环路产生，由

于以太网、令牌环网等第二层协议均没有控制环路数据帧的机制，因此各小型环路产生的广播风暴将不断扩散到全网，进而造成网络瘫痪。

与广播概念相类似的还有组播（Multicast，或称多播），组播是一点对多点的通信，是一种比较有效的节约网络带宽的方法。例如在视频点播等多媒体应用中，当把多媒体信号从一个节点传输到多个节点时，采用广播方式会浪费带宽，重复采用点对点传播也会浪费带宽，而组播能够把帧发送到组地址，而不是单个主机，也不是整个网络。由于它的发送范围明显小于广播，因而减少了对网络带宽的占用。

网络运行时，应当了解网络里所运行的所有协议以及这些协议的主要特点，这样才能更有利于对广播信息流量的控制。通常，交换机对网络中的广播帧或组播帧不会进行任何数据过滤，因为这些地址帧的信息不会出现在 MAC 层的源地址字段中。交换机总是直接将这些信息广播到所有端口[1]，如果网络中存在环路，这些广播信息将在网络中不停地转发，直至导致交换机出现超负荷运转(如 CPU 过度使用，内存耗尽等），最终耗尽所有带宽资源、阻塞全网通信

通过使用第三层的路由设备（详见本书的后半部分），能够很好地解决广播风暴问题。当客户端发出用来查询的广播包时，路由器能够将其截获并判断是否进行全网转发，从而大大抑制了引发广播风暴连锁反应的可能性。

由于路由器能够有效隔离广播域，因此，一些局域网就设计成以路由器为中心的网络构架。但是，路由器通常又会成为网段（子网）间通信的瓶颈。实际上，目前一些交换机就具备一定程度的广播风暴控制功能，只要配置合理，就不会出现环路引起的广播风暴。比较高端的设备如第三层交换机，在这方面则具有很好的性能。

Cisco 第二层交换机也支持这种广播风暴控制功能。它定义交换机端口的广播门限值，当端口接收的广播超过了该值时，该端口便会立刻处于挂起状态以避免出现循环广播状态。该功能默认值为禁用，需要通过手动配置打开。

2. 多个广播帧副本

网络中如果存在环路，目的主机可能会收到某个广播帧的多个副本，此时会导致上层协议在处理这些数据帧时无从选择，产生迷惑：究竟该处理哪个帧呢？

严重时还可能导致网络连接的中断，同时引起 MAC 地址数据库的混乱。

当交换机连接不同网段时，将会出现通过不同端口接收到同一个广播帧的多个副本的情况。这一过程也会同时导致 MAC地址表的多次刷新，这种持续的更新、刷新过程会严重耗用内存资源，影响该交换机的交换能力，同时降低整个网络的运行效率。严重时，将耗尽整个网络资源，并最终造成网络瘫痪。

1.5 生成树协议

要实现冗余备份，提高网络的可靠性，必须解决环路拓扑结构为网络带来的以上两种致命的负面影响。

生成树协议(Spanning-Tree Protocol, STP）最初是由美国数字设备公司（Digital Equipment Corp, DEC)开发的，后经电气电子工程师学会(Institute of Electrical and Electroric Engineers, IEEE)进行修改，最终制定了相应的 IEEE802.1d 标准。STP协议的主要功能就是为了

解决由于备份连接所产生的环路问题。

STP 协议的主要思想就是当网络中存在备份链路时，只允许主链路激活，如果主链路因故障而被断开后，备用链路才会被打开。

注意，虽然 DEC 和 IEEE 的 STP 协议的设计目标相同，都是为了解决网络环路问题，但二者的使用并不兼容。

1.5.1 STP 协议原理

STP 的基本做法就是生成“一棵树”，树的根是一个称为根桥的交换机。

根据设置不同，不同的交换机会被选为根桥，但任意时刻只能有一个根桥。由根桥开始，逐级形成一棵树，根桥定时发送配置数据包，非根桥接收配置数据包并转发，如果某台交换机能够从两个以上的端口接收到配置数据包，则说明从该交换机到根的路径不止一条，这样便构成了循环回路。

此时交换机就根据端口的配置选出一个端口并把其他的端口阻塞，消除循环。当某个端口长时间不能接收到配置数据包的时候，交换机认为该端口的配置超时，网络拓扑可能已经改变。此时就重新计算网络拓扑，重新生成一棵树。

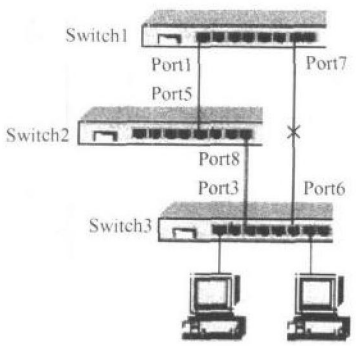


图 1.5 由 STP 协议构成的网络

1. STP 修剪与 BPDU

STP 协议通过使用 STP 算法来动态地探测网络中存在的环路，自动调整网络中的备份路径，并及时控制其进入备份状态。此外，使用 STP 协议还可以迅速改变或调整网络当前的拓扑结构，并最终将网络的现有拓扑修剪成树状结构，即只有主干与分支部分而不会形成环路，就像一颗树一样，这称之为 STP 修剪。图 1.5 所示为一使用 STP 协议构成的网络连接，从图中看到，在主交换机链路工作时，备份交换机链路(Port6 ~ Port7)则处于暂时禁用状态。

STP 协议是通过在网络中发送和接收桥协议数据单元（Bridge Protocol Data Unit，BPDU）帧来进行网络调整的，BPDU 的配置信息在网络中以组播的方式传播，其中每个设备的 ID 号都可以通过 BPDU 帧发送到其他设备。

2. 根桥的选举

经过 STP 修剪完的树状结构里，只存在一个惟一的树根（Root），这树根可以是一台网桥或一台交换机，称之为根桥，由它作为核心基础来构成网络的主干与其他分支结构。尽管根桥由 STP 协议自动选举产生，但其的选择非常重要，选举根桥的原则应当了解：

a. 根桥必须具有最低的优先权 ID 与 MAC 地址。Cisco 交换机的 ID 值为 32 768，在优先权数值相等时，将由 MAC 地址大小来决定。谁的 MAC 地址值低就由谁来作为根设备 。

b. 在运行 STP 协议的交换机上，端口分为已分配端口与未分配端口两种类型。

已分配端口此时端口牌处于激活状态。实际上由于根设备的所有端口是构成主干网络的基础，因此根设备的所有端口类型都将处于已分配状态，而牌其他位置的设备

端口状态要由 STP 算法决定。每个端口都有一个关于路径长度的默认值，可以手动进行调整或是依据 STP 算法自动生成一个路径长度值。这处路径的长度值越小，它的效率就越高，也就会成为最优路径，此时这个端口就会被激活而处于已分配状态。

- 未分配端口未分配端口实际上就是处于备份状态。该设备端口由于具有较大的路径长度值而被 STP 算法关闭，使其处于未分配状态。当端口处于未分配状态时，这些端口的链路便不会进行数据传输。只有当某一已分配的端口发生故障时，端口类型才会由未分配类型自动变成已分配类型。

1.5.2 STP 的端口状态

STP 端口存在以下几种不同状态，见表 1.3。

表 1.3 STP 端口的不同状态

状　态	属　性
禁用(Disabled)	不能接收 BPDU 信息，不能转发数据
阻塞(Blocking)	可接收 BPDU 信息，不能转发数据
侦听(Listening)	可监听和接收 BPDU 信息，不能转发
学习(Learning)	可接收和发送 BPDU 信息，建立 MAC 地址表，不能转发数据
转发(Forwarding)	可与其他交换机交换 BPDU 信息，可转发数据

a. 禁用此种状态下无法对端口进行操作。端口不能接收 BPDU 信息，更不能进行数据信息的转发。

b. 阻塞此种状态下可以对端口进行操作。端口可以接收 BPDU 信息，但却不能转发数据。这是因为该端口相对于其他端口有较大的路径长度值，为了避免形成环路，STP 将其置于阻塞状态。

c. 侦听此种状态下可以对端口进行操作。端口可以接收 BPDU 信息，但它不具有 BPDU 信息的转发与 MAC 地址的学习能力。每当网络拓扑结构发生改变时，端口便会立即进入这种状态。它监听网络上的 BPDU 信息以便随时准备进入学习状态。

d. 学习此种状态下可以对端口进行操作。端口可以主动地接收和发送 BPDU 数据信息，负责建立 MAC 地址表并使之与相应的端口进行一一映射，但同样不能转发数据信息。只有当侦听到网络拓扑结构发生改变时，端口才会进入这种状态。

e. 转发此种状态下可以对端口进行操作。端口可以转发数据信息，并与其他交换机交换 BPDU 信息以获得最佳的路径长度值，完成网络拓扑结构的调整。

从上面的状态信息可以看到，这是交换机的某个端口从不可用状态转变成可用状态的过程。当交换机完成初始化后，为避免形成环路，STP 会使一些端口（备份链路的端口）直接进入阻塞状态。当网络中主链路发生故障时，网络的拓扑结构即会发生变化，处于阻塞状态的端口就会通过 BPDU 了解（侦听）到这变化，端口的状态就会立刻从阻塞状态转变到学习状态，完成 MAC 地址表的建立后成转发状态，并在转变过程中经历侦听与学习两个状态，最终转为正常的工作模式。

一个端口从禁用状态到转发状态通常需要经历 50s 时间，这样才能保证 STP 拥有足够的时间来了解整个网络的拓扑结构。

第 2 章　Cisco IOS 与交换机的基本配置

知识要点：

可管理的交换机也就是一台专用的计算机，必须有操作系统软件才能工作。对交换机的管理和配置就是调用其操作系统软件，通过命令行或图形界面来进行的。

交换机的操作系统软件，固化在其 ROM 和 Flash ROM 中。Cisco 公司的大部分系列的交换机操作系统软件为 Cisco IOS。

Cisco IOS 内置的命令行解释器，通过一系列的配置命令实现对交换机的全部管理功能.

命令行解释器有多种命令模式，用于管理的安全性和实现不同的管理功能。

配置交换机可以通过其配置口进行，也可通过其 Ethernet 口进行。

交换机的最基本的配置包括其主机名、口令和 IP 地址的配置等。

思科(Cisco)公司是世界最大的网络设备供应商之一，其交换机和路由器的销售占有最高的市场份额，技术处于领先的地位。Cisco 绝大部分系列交换机和路由器的操作系统软件都使用 Cisco 网际操作系统（Cisco Inter-network Operating System, Cisco IOS)。个别较老的系列使用 SET 命令集。路由器中可以使用全部的 IOS 命令，交换机中有少部分 IOS 命令不能用。

2.1　CLI 命令行解释器

Cisco IOS 内置 Web 浏览器和命令行解释器(CLI),使用 Web 能实现部分配置管理功能，界面友好直观。而全部配置管理功能则使用 CLI 实现。

1. CLI 命令模式

不同的命令需要在不同的命令模式下才能执行，Cisco 网络操作系统常使用 6 种命令模式：

- 普通用户(User EXEC)模式
- 特权用户(Privileged EXEC)模式
- 全局配置(Global configuration)模式
- 接口配置(Interface configuration)模式
- 虚拟局域网参数配置(VLAN database) 模式
- 进程配置(Line configuration)模式

在不同的模式下,CLI 界面的提示符不同。表 2.1 列出了该 6 种命令模式的用途、提示符、访问方式和退出方法。

表 2.1 命令模式摘要

模式	访问方法	提示符	退出方法	用途
普通用户(User EXEC)模式	一个进程的开始	router >	键入 logout 或 quit	改变终端设置执行基本测试显示系统信息
特权用户(Privileged EXEC)模式	在 User EXEC 模式中键入 enable 命令	router #	键入 disable 退出	校验键入的命令,该模式由密码保护
全局配置(Global configuration)模式	在 Privileged EXEC 模式中键入 configure terminal 命令。	router(config)#	键入 exit 或 end 或按下 ctrl-z,返回至 Privileged EXEC 状态	将配置的参数应用于整个交换机
端口配置(Interface configuration)模式	在 Global configuration 模式中,键入 interface 命令	router(config-if)#	键入 exit 返回至 Global configuration 模式,按下 ctrl-z 或键入 end,返回至 Privileged EXEC 模式	为 ethernet interfaces 配置参数
虚拟局域网参数配置(VLAN database)模式	在 Privileged EXEC 模式中键入 vlan database 命令	router{vlan}#	键入 exit,返回到 Privileged EXEC 模式	配置 VLAN 参数
进程配置(Line configuration)模式	在模式 Global configuration 中为 line vty or line console 命令指定一行	router{config-line}#	键入 exit 返回至 Global configuration 模式按下 ctrl-z 或键入 end ,返回至 Privileged EXEC 模式	为 terminal line 配置参数

2. 命令模式的使用

CLI 之所以采用多种命令模式是为了保护系统的安全。

命令行采用分级保护方式，防止未经授权非法侵入。所有命令被分组，每组分属不同命令模式，某个命令模式下只能执行所属的命令。当然，有的常用命令也出现在多个模式下。

各命令模式之间可以切换。如在普通用户模式提示符下键入“enable”,就可进入特权用户模式。特权用户模式是进入其他用户模式的“关口”，欲进入其他用户模式，必须先进入特权用户模式。CLI 提供进入特权用户模式的口令保护。

1) 普通用户模式

路由器启动后直接进入该模式，该模式只包含少数几条命令，用于查看交换机或路由器简单运行状态和统计信息。

2) 特权用户模式

该模式由口令保护，用户进入该模式后可查看交换机或路由器的全部运行状态和统计信息，并可进行文件管理和系统管理。而且，特权用户模式是进入其他用户模式的“关口”，欲进入其他用户模式，必须先进入特权用户模式。

在普通用户模式下键人命令 enable,即可进入该模式。

3) 全局配置模式

在该模式下可配置交换机或路由器的全局参数，如主机名、密码、路由协议等。在特权用户模式下键人命令 config terminal,即可进入该模式。

4）端口配置模式

该模式可对交换机或路由器的各种端口进行配置，如配置 IP 地址，封装网络协议等。

在全局配置模式下键人命令 interface interface-type，即可进入端口配置模式，其中 interface-type 为具体的端口名称,如 ethernet 1。

5）虚拟局域网参数配置模式

在该模式下可对交换式网络进行虚拟局域网的划分。

在特权模式下键人命令 vlan database，即可进入虚拟局域网参数配置模式。

6）进程配置模式

在该模式下可为使用终端仿真程序配置交换机或路由器设置进程号。

在全局配置模式下键人命令 line vty line-number ,其中 line-number 为进程号。

交换机本身不带输入输出设备(如键盘、显示器),只有通过终端设备或普通的计算机来实现对其网络操作系统的访问，从而对其配置和管理。

2.2 配置交换机的方法

配置交换机，方法之一是使用 Console 线把计算机直接连接到 Console 端口 方法之二是通过网络计算机以 Telnet 方式进行。还可通过 Web 或网管软件对交换机进行一些基本的配置和管理。此外,还可通过 TFTP 服务器实现对交换机软件系统的保存、升级、配置文件的保存和下载等。

1. 通过配置(Console) 口

交换机的配置口是一串行口，将其与计算机的串口通过专用的配置 (Console)电缆连接起来,实现对交换机的配置,具体步骤如下。

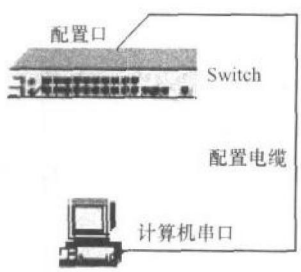


图 2.1 通过配置口配置交换机

1）建立配置环境

如图2.1 所示,把已安装超级终端程序的 Windows 98 计算机用 Console 电缆与交换机的 Console 口连接起来。

2）在 Windows 98 中运行并设置超级终端

a. 单击“ 开始 ”,指向“ 程序 ”,指向“ 附件 ”,指向“ 通讯 ”,然后单击“ 超级终端 ”,弹出“ HyperTerminal” 对话框。双 击“Hypertrm ’图标,弹出如图 2.2 所示的对话框。

b. 给连接选取图标、取名后单击“ 确定 ’按钮,出现如图 2.3 所示的对话框，根据实际所用的计算机串口号选择“ 连接时使用 ’的端口。

c. 设置端口参数为波特率 9 600b/s、8 位数据位、1 位停止位、无校验和无流控,如图 2.4 所示。

3）给交换机上电

开启交换机电源开关，接连按回车，在计算机屏幕上即可显示交换机初始界面：

```
Cisco Systems, Inc. Console
Enter password:
```

输入正确的口令并回车，即可登录到交换机。就可以以图形界面或 CLI 方式对交换机进

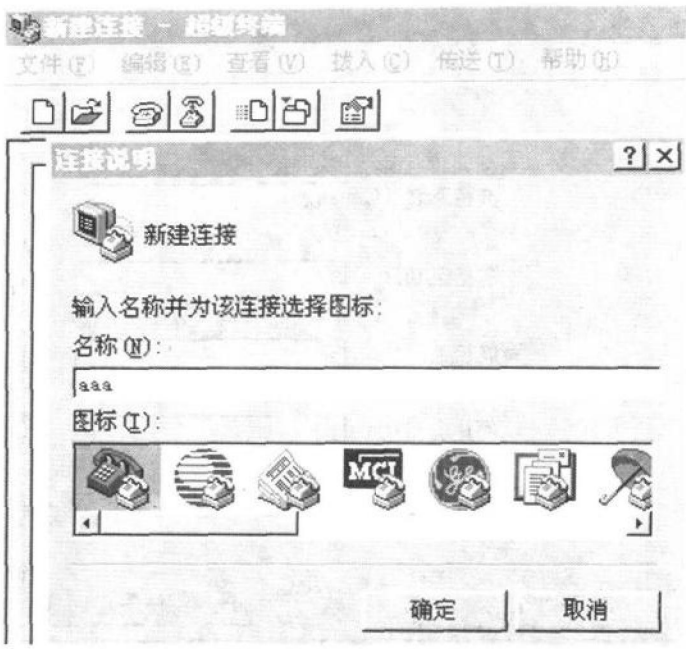


图 2.2 新建一个超级终端连接

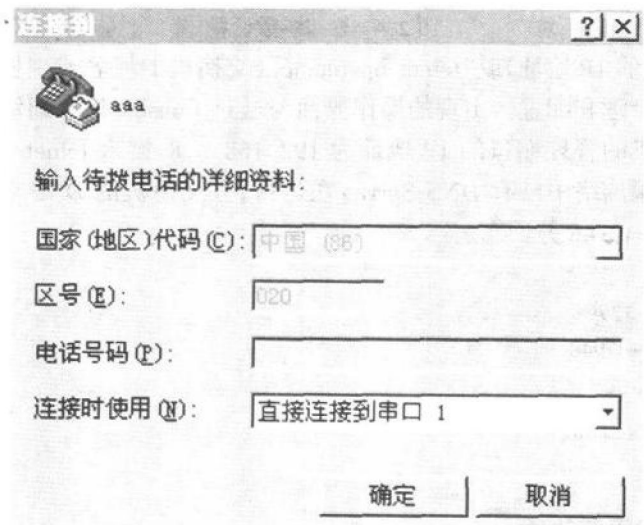


图 2.3 新建连接使用的端口

行配置和管理了。

2. 通过 Telnet

1) 配置环境的建立

把计算机与交换机的某 Ethernet 端口(通常是 100Mb/s 端口或 1 000Mb/s 端口,该端口称为管理端口)用 RJ45 连接线连接起来,交换机的该端口应已经设置了 IP 地址。

2) 运行终端仿真程序 Telnet

Windows 9x /Me, Windows NT/ 2000 操作系统上都有 Telnet 终端仿真程序。当交换机设置为允许远程访问时,可以在网络上任何一台与之相连的计算机上执行“ telnet ip-address”

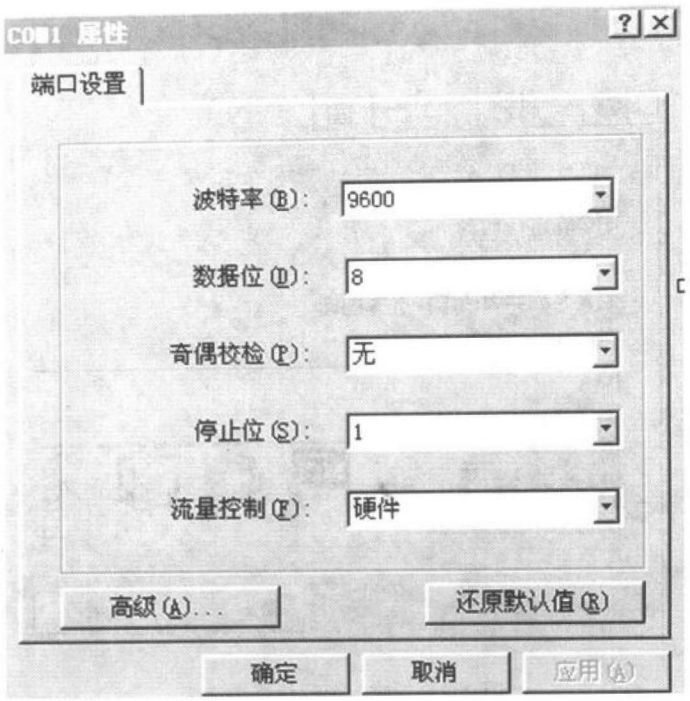


图2.4 端口参数设置

(交换机的管理端口的 IP 地址)或‘ telnet hostname”(交换机的域名或主机名)命令,登录至该交换机并对其进行管理和配置。出现的操作界面与通过 Console 口以超级终端进行连接时完全相同。例如交换机的管理端口的 IP 地址为 192.168.0.8,键入 telnet 192.168.0.8 即可登录到该交换机。如果网络中已有 DNS Server 在运行,且交换机的 DNS 名字为 Catalyst2948,则键入 telnet Catalyst2948 并回车。

屏幕显示:

```
Trying 172.68.16.129…
Connected to Catalyst2948.
Escape character is ']'
Cisco Systems Console
Enter password:
```

3. 通过 Web 或网管软件

通过 Web 浏览器可在网络中对交换机进行远程管理。但通过该方式管理前,必须已经完成交换机 IP 地址的设置,并且将交换机和管理计算机连接在同一 IP 网段。

运行 Web 浏览器,在 IP 地址栏中键入欲管理的交换机的 IP 地址或域名后回车,在弹出的对话框中键入具有最高权限的用户名和密码(对交换机的访问通常必须设置权限)即可进入交换机管理的主 Web 界面,进行一些基本的配置和管理。

使用网管软件如 Cisco Works 或 Cisco View ,也可对路由器进行管理。

4. 使用 TFTP 服务器

任何一台计算机只要安装有 TFIP{Trivial File Transfer Protocol} 服务器软件,即可成为

TFIP 服务器。TFTP 服务器可实现交换机或路由器软件系统的保存、升级，配置文件的保存和下载，这使得对交换机的管理变得简单和快捷。因此，在进行交换机的管理前，最好先安装一台 Cisco TFTP 服务器。TFTP 服务器软件可到 Cisco 的网站 http://www.cisco.com 或 http://www.ciscostation.com 下载。Cisco IOS 系统软件也可在此网站下载。把软件映像复制到该 TFTP 服务器根目录下（c: \ Program files \ cisco systems \ cisco tftp server），通过该 TFTP 服务器，即可实现对交换机或路由器软件的升级，以及配置文件的备份与恢复。

2.3 交换机的基本配置

配置交换机的主机名、口令和端口 IP 地址，以及 Telnet 进程等，称为交换机的基本配置。

1. 配置主机名与口令

配置交换机的主机名和口令，操作如下：

进入 enable 模式：

```
router > enable
router #
```

进入 Global configuration 模式：

```
router # configure terminal
router(config) #
```

设置主机名，使用命令 hostname，后跟欲为交换机命名的名称字符串，如“catalyst”：

```
router(config) # hostname catalyst
catalyst(config) #
```

设置 password，password 为非加密密码。使用命令 enable password，后跟欲做密码的字符串，如 asD # 11p，用在版本 Cisco IOS10.2 及以下：

```
catalyst(config) # enable password asD # 11p
```

设置 secret 密码，secret 为加密密码。使用命令 enable secret，后跟欲做密码的字符串，如 sji98A，用在版本 Cisco IOS 10.3 及以上：

```
catalyst(config) # enable secret sji98A
```

注意这两种密码都对大、小写敏感。

2. 配置端口 IP 地址和终端线路的 Telnet 进程管理

配置端口 IP 地址，主要是便于使用此端口对交换机进行管理，该端口称为管理端口。通常是把快速以太网端口（100Mb/s Fast Ethernet，用 f 后跟数字编号表示，如 f1 表示第 1 个快速以太网端口）或千兆位以太网端口（1 000Mb/s Gigabit Ethernet，用 g 后跟数字编号表示，如 g49 表示编号为 49 的一个千兆位以太网端口）作为管理端口。通过终端线路的 Telnet 进程管理配置，可设定对交换机的登录权限，增强交换机的安全性。

1）配置端口 IP 地址

进入 Interface configuration 模式。如欲配置 f1 端口，则：

```
catalyst(config) # interface f1
catalyst(config-if) #
```

为该 Fast Ethernet 端口键入 IP 地址和子网掩码。使用命令 ip address，后跟 IP 地址和子