

交换机的基本配置

- 主要内容：
 - 了解交换机工作原理与堆叠连接方法
 - 掌握交换机的主机名配置
 - 掌握交换机IP地址配置
 - 掌握交换机的口令安全性配置

交换机工作原理与堆叠连接方法

- OSI参考模型第二层交换
- 生成树协议
- 交换机的3种交换方式

OSI参考模型第二层交换

局域网交换技术是作为对共享式局域网提供有效的网段划分的解决方案而出现的，它可以使每个用户尽可能地分享到最大带宽。交换机工作在OSI七层网络模型中的数据链路层，因此交换机对数据包的转发是建立在MAC（Media Access Control）地址基础之上的，对于IP网络协议来说，它是透明的，即交换机在转发数据包时，不知道也无须知道信源机和信宿机的IP地址，只需知其物理地址即MAC地址。

OSI参考模型第二层交换

交换机在操作过程当中会不断的收集信息去建立MAC地址表，MAC地址表说明了某个MAC地址是在哪个端口上被发现的，所以当交换机收到一个TCP / IP数据包时，它会查看该数据包的目的MAC地址，然后核对自己的MAC地址表以确认应该从哪个端口把数据包发出去。这功能由ASIC(Application Specific Integrated Circuit)进行，因此速度相当快，一般只需几十微秒，交换机便可决定一个IP数据包该往那里送。

OSI参考模型第二层交换

当交换机收到一个目标地址未知的数据包，就是说目的MAC地址不能在其MAC地址表中找到时，交换机会把IP数据包从它每一个端口中送出去。

交换机的特性

- 地址学习,
- 转发或过滤
- 避免循环

地址学习

以太网交换机能够通过读取传送包的源——MAC地址和记录帧进入交换机的端口来学习网络上每个设备的地址。然后，交换机把该信息加到它的转发数据库。地址是动态学习的。这意味着，当读取新MAC地址时它们被学习并存储在CAM（Content-Addressable Memory，内容可寻址存储器）。当在CAM中，没有找到的源被读取时，它被学习并存储以备将来使用。

每次存储地址时，地址被打上时间标记，那些一段时间内还没有被引用的地址从列表中移走，通过移走过时的或老的地址。CAM维护了一个精确和有用的转发数据库。

转发或滤除

当主机A发一个帧给主机B时，由于目的MAC地址（主机B的MAC地址）已在MAC地址表中存在对应项，故交换机将此帧直接发到B所在交换机的端口。而且交换机不会再将帧发往其它端口，这样就节省了其它端口上的带宽。这就是所谓的转发与过滤。

但是对于广播和组播，交换机通常是把广播帧或组播帧向所有端口转发，不管MAC地址表是否完整。而一个交换机永远学习不到广播或组播地址，因为它们永远不会出现在一个帧的源地址中。

所以第二层的交换机无法控制广播域，用交换机分割的网段虽然处于不同的冲突域中，但仍然处于同一个广播域中。因此，需要第三层设备（如路由器）来分割广播域。

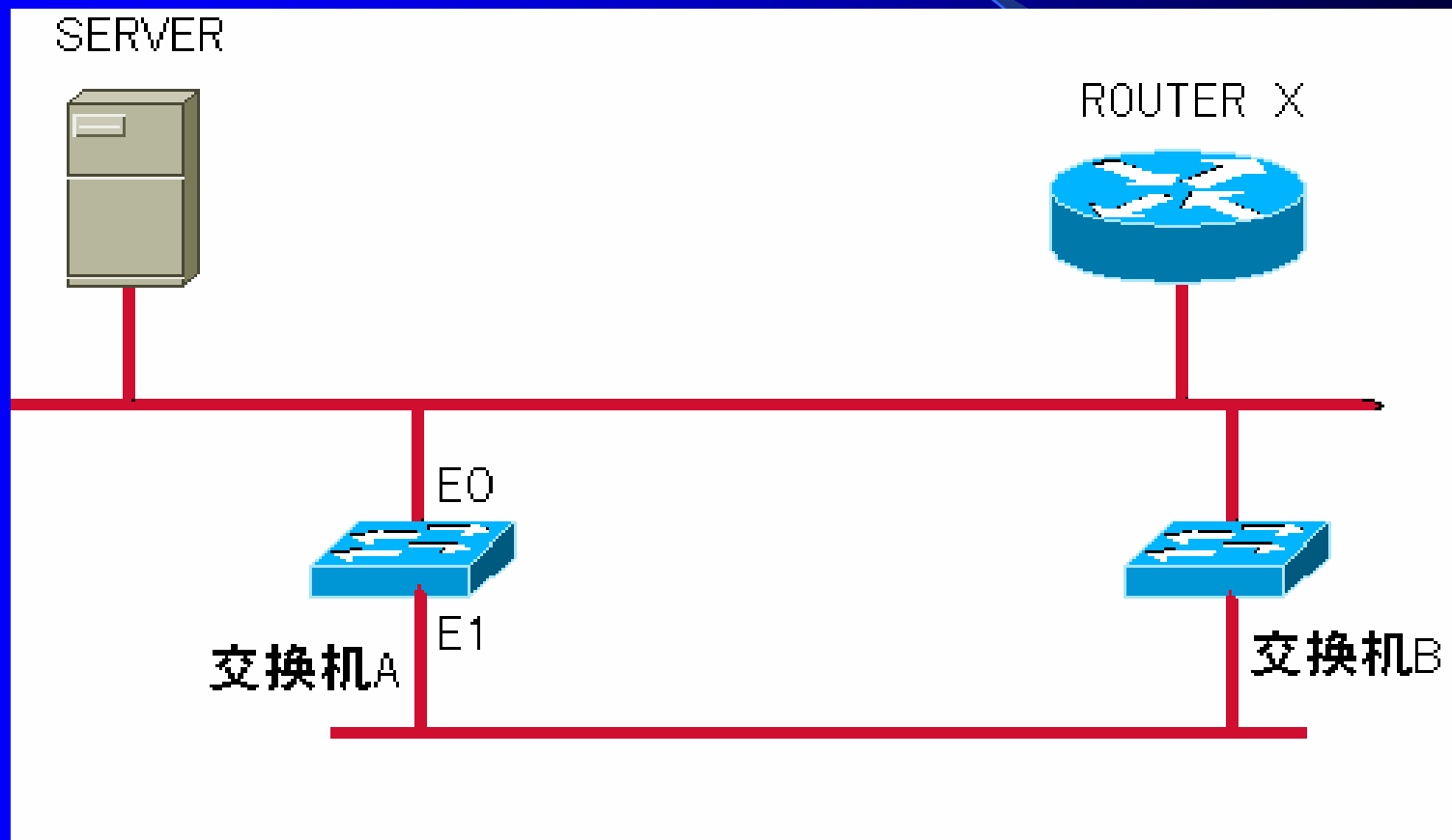
避免循环

在网络设计中，冗余链路通常是必不可少的。因为使用单一链路，万一发生断路可能会使整个网络陷入瘫痪的窘境。

但问题是，事物总是一分为二的，冗余路径也带来了很多问题。

- 广播风暴。
- 重复帧拷贝。
- MAC地址表表项不稳定。

广播风暴

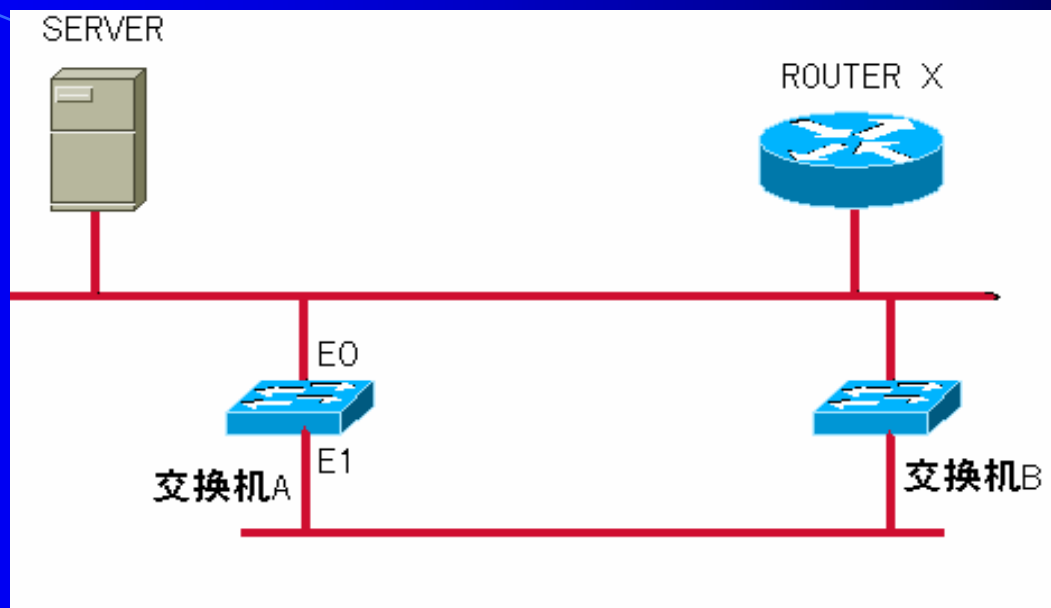


广播风暴

当服务器想知道默认网关（路由器X）的MAC地址时，会起用ARP。那么一个ARP帧就是一个广播帧（目的MAC地址为全1）。当交换机A收到后此帧就会转发到网段2上。当交换机B收到后，又转发到网段1上，形成循环，这就是广播风暴，并且是双向循环。这极大的浪费了网络资源。

避免循环机制可以通过阻塞（逻辑上）其中某一端口（不允许接收帧和发送帧）来消除广播风暴问题

重复帧拷贝



由于冗余路径的存在，主机可能会从不同的路径接收到相同的帧，造成资源的浪费。

MAC地址表表项不稳定

如果交换机A要传送帧个服务器，就可能会产生困惑，因为从端口E0发送可以到达，从端口E1发送也可到达。由于冗余链路导致MAC地址表的表项不惟一，从而使交换机有可能不转发此帧，或者重复发送到不同端口，造成主机A收到多份拷贝。这也是对网络资源的浪费。

生成树协议

- 生成树协议的作用与原理
- 生成树操作
- 根网桥选举
- 路径花费
- 生成树的端口状态
- 汇聚

生成树协议的作用与原理

STP（生成树协议）的主要任务是防止2层的循环，STP使用生成树算法（spanning-tree algorithm，STA）来创建一个拓扑数据库，然后查找出冗余连接并破坏它。

生成树操作

前面说过：STP的任务就是查找出网络中的所有连接，关闭一些会造成循环的冗余连接。STP首先选举1个根桥，用来对网络中的拓扑结构做决定。当所有的switches认同了选举出来的根桥后，所有的bridge开始查找根端口。假如在switches之间有许多连接，只能有1个端口作为指定端口。

根网桥选举

bridge ID用来在STP域里选举根桥和决定根端口，这个ID是8字节长，包含优先级和设备的MAC地址，IEEE版本的STP的默认优先级是32768，决定谁是根桥。假如优先级一样，那就比较MAC地址，MAC地址小的作为根桥。

路径花费

生成树的路径花费是在路径上所有链路的路径花费总和，这是由链路带宽决定的。

生成树的端口状态

运行STP的交换机端口的5种状态：

- 堵塞(blocking):不转发帧,只监听BPDU,主要目的是防止循环的产生.默认情况下,当switch启动时所有端口均为blocking状态；
- 监听(listening):端口监听BPDU,来决定在传送数据帧之前没有循环会发生；
- 学习(learning):监听BPDU和学习所有路径,学习MAC地址表,不转发帧；
- 转发(forwarding):转发和接收数据帧；
- 禁用(disabled):不参与帧的转发和STP,一般在这个状态的都是不可操作的。

汇聚

汇聚,也叫收敛(convergence):当所有端口移动到非转发或堵塞状态时,开始收敛,在收敛完成前,没有数据将被传送。收敛保证了所有的设备拥有相同的数据库达到一致。一般来说从堵塞状态进入到转发状态需要50秒。

交换机的3种交换方式

- 存储 - 转发式交换方式
- 直通式交换方式
- 消除片断式（改良直通式）交换方式

存储 - 转发式交换方式

存储-转发（Store and Forward）是计算机网络领域使用得最为广泛的技术之一，以太网交换机的控制器先将输入端口到来的数据包缓存起来，先检查数据包是否正确，并过滤掉冲突包错误。确定包正确后，取出目的地址，通过查找表找到想要发送的输出端口地址，然后将该包发送出去。正因如此，存储转发方式在数据处理时延时大，这是它的不足，但是它可以对进入交换机的数据包进行错误检测，并且能支持不同速度的输入/输出端口间的交换，可有效地改善网络性能。它的另一优点就是这种交换方式支持不同速度端口间的转换，保持高速端口和低速端口间协同工作。实现的办法是将10Mbps低速包存储起来，再通过100Mbps速率转发到端口上。

直通式交换方式

Cisco称这种模式叫cut-through, fastforward或者real time模式, 使用这种模式的时候, LAN switch只读取到帧的目标地址为止, 减少延时, 但是不适合与高偏向错误率的网络。

直通式交换方式

它在输入端口检测到一个数据包时，检查该包的包头，获取包的目的地址，启动内部的动态查找表转换成相应的输出端口，在输入与输出交叉处接通，把数据包直通到相应的端口，实现交换功能。由于它只检查数据包的包头（通常只检查14个字节），不需要存储，所以切入方式具有延迟小，交换速度快的优点（所谓延迟（Latency）是指数据包进入一个网络设备到离开该设备所花的时间）。

直通式交换方式

它的缺点主要有三个方面：一是因为数据包内容并没有被以太网交换机保存下来，所以无法检查所传送的数据包是否有误，不能提供错误检测能力；第二，由于没有缓存，不能将具有不同速率的输入/输出端口直接接通，而且容易丢包。如果要连到高速网络上，如提供快速以太网（100BASE - T）、FDDI或ATM连接，就不能简单地将输入/输出端口“接通”，因为输入/输出端口间有速度上的差异，必须提供缓存；第三，当以太网交换机的端口增加时，交换矩阵变得越来越复杂，实现起来就越困难。

消除片断式（改良直通式）交换方式

这种模式和cut-through类似，但是，LAN switch读取到数据（data）部分的前64字节是Catalyst 1900的默认模式。

消除片断式（改良直通式）交换方式

这是介于直通式和存储转发式之间的一种解决方案。它在转发前先检查数据包的长度是否够64个字节（512 bit），如果小于64字节，说明是假包（或称残帧），则丢弃该包；如果大于64字节，则发送该包。该方式的数据处理速度比存储转发方式快，但比直通式慢，但由于能够避免残帧的转发，所以被广泛应用于低档交换机中。

消除片断式（改良直通式）交换方式

使用这类交换技术的交换机一般是使用了一种特殊的缓存。这种缓存是一种先进先出的FIFO（First In First Out），比特从一端进入然后再以同样的顺序从另一端出来。当帧被接收时，它被保存在FIFO中。如果帧以小于512比特的长度结束，那么FIFO中的内容（残帧）就会被丢弃。因此，不存在普通直通转发交换机存在的残帧转发问题，是一个非常好的解决方案。数据包在转发之前将被缓存保存下来，从而确保碰撞碎片不通过网络传播，能够在很大程度上提高网络传输效率。

交换机堆叠连接方法

当网络规模增长时，固定端口交换机的扩展能力会受到制约。

为了使交换机满足大型网络对端口的数量要求，一般在较大型网络中都采用交换机的堆叠方式来解决。要注意的是只有可堆叠交换机才具备这种端口，所谓可堆叠交换机，就是指一个交换机中一般同时具有"UP"和"DOW"堆叠端口。当多个交换机连接在一起时，其作用就像一个模块化交换机一样，堆叠在一起交换机可以当作一个单元设备来进行管理。一般情况下，当有多个交换机堆叠时，其中存在一个可管理交换机，利用可管理交换机可对此可堆叠式交换机中的其他“独立型交换机”进行管理。

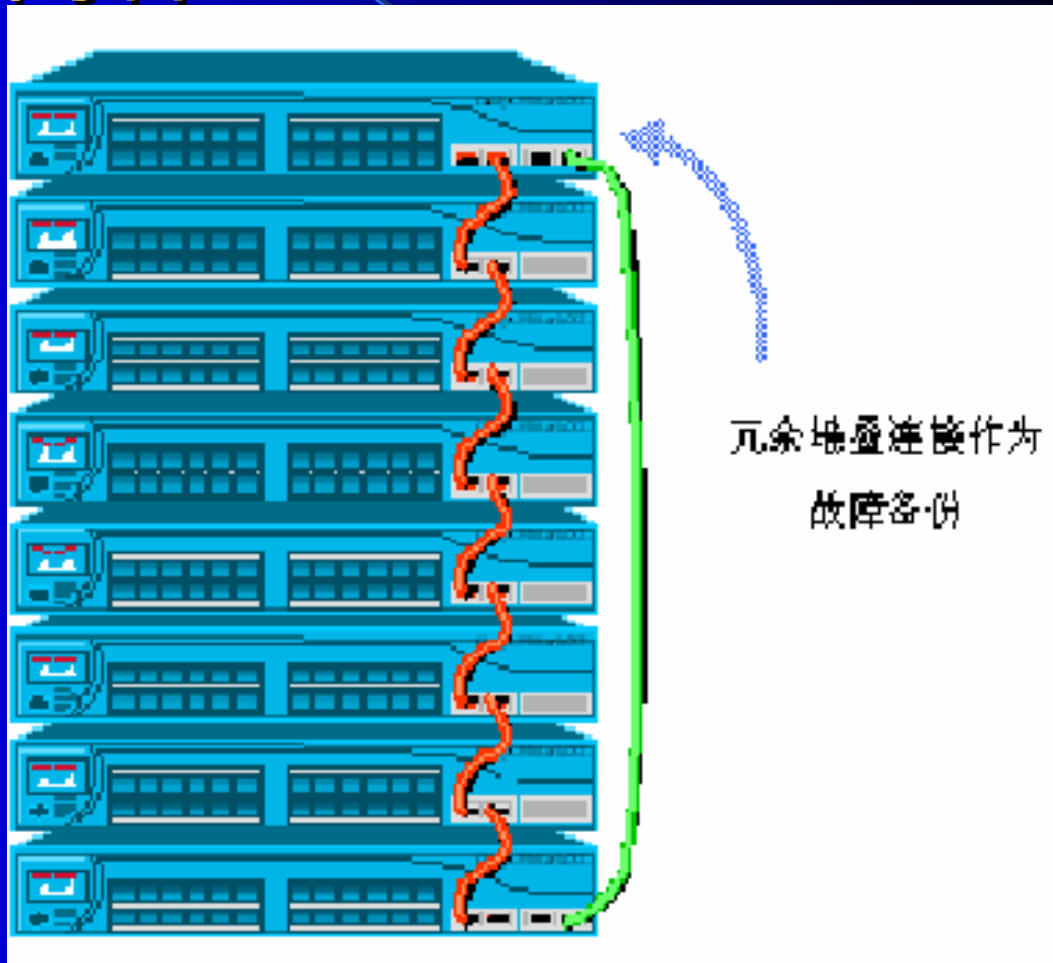
交换机堆叠连接方法

堆叠中的所有交换机可视为一个整体的交换机来进行管理，也就是说，堆叠中所有的交换机从拓扑结构上可视为一个交换机。堆栈在一起的交换机可以当作一台交换机来统一管理。交换机堆叠技术采用了专门的管理模块和堆栈连接电缆，这样做的好处是，一方面增加了用户端口，能够在交换机之间建立一条较宽的宽带链路，这样每个实际使用的用户带宽就有可能更宽（只有在并不是所有端口都在使用情况下）。另一方面多个交换机能够作为一个大的交换机，便于统一管理。

可堆叠交换机常用的堆叠方式有两种：

- 菊花型

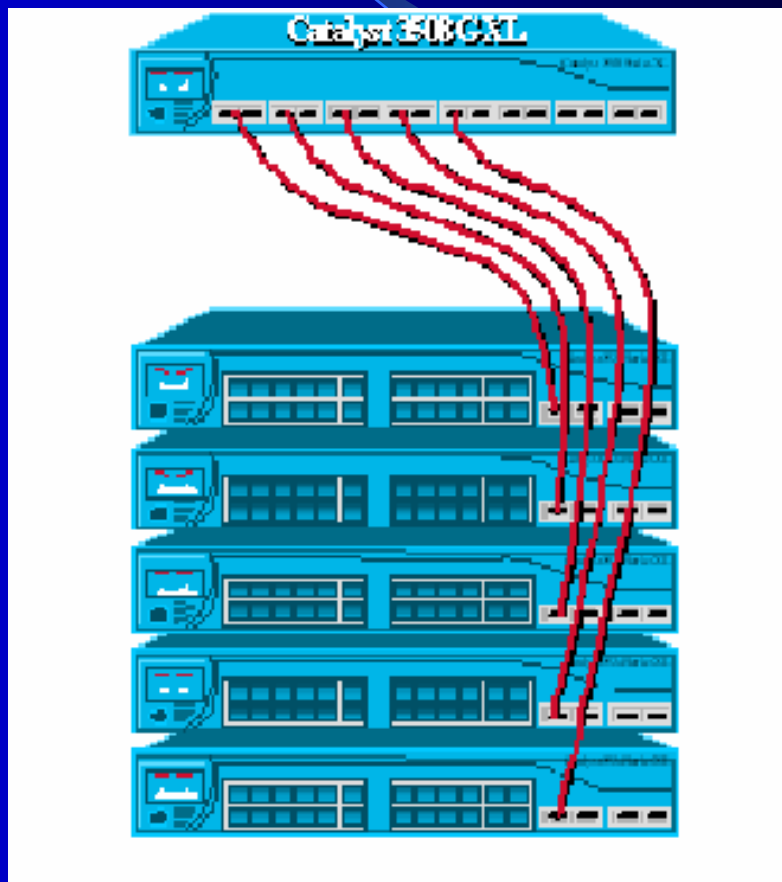
菊花型堆叠要求堆叠交换机通过堆叠接口或模块首尾相连，是一种类似于普通的交换机之间级联连接，通过相对高速的端口串接和软件的支持，最终实现构建一个多交换机的层叠结构。



可堆叠交换机常用的堆叠方式有两种：

- 星型

星型堆叠是需要一个主交换机，其它是从交换机，每台从交换机都通过堆叠接口或模块与主交换机相连。这种方式要求主交换机的交换容量（背板带宽）要比从交换机的要大。



交换机的主机名配置

所有出厂的交换机都有默认的配置和默认的系统名称或者提示。可以更改这个名字，便于每一台交换机在园区网中能够惟一的进行认证。

交换机的主机名配置

为了改变主机或者系统的名称，输入配置模式中如下的命令：

```
Switch (config) # hostname hostname
```

主机名称是一个1到255个字母或者数字组成的字符串。一旦执行这条命令，系统做出改变提示，反映新的主机名称。

交换机的主机名配置

给1900配置主机名，执行hostname命令，如下：

```
>(config)#hostname Noko  
Noko(config)#
```

交换机的主机名配置

给2950配置主机名，执行hostname命令，如下：

```
Switch(config)#hostname Noco
```

```
Noco(config)#
```

交换机IP地址配置

- 工作在第二层的交换机IP地址配置
- 工作在第三层的交换机IP地址配置

工作在第二层的交换机IP地址配置

在默认情况下，交换机仅允许用户通过控制台端口进行访问。即一台交换机操作在第2层，交换机超级用户处理机出于管理目的，仍然必须在第3层维护一个IP栈。然后，可以给交换机分配IP地址和子网掩码，使得与交换机超级用户进行远程通信成为可能。

工作在第二层的交换机IP地址配置

可以在全局配置模式下执行如下的命令，为管理VLAN（默认情况下是VLAN1分配IP地址）。

```
Switch (config) # interface vlan vlan-id
```

```
Switch (config-if) # ip address ip-address netmask
```

```
Switch (config-if) # ip default-gateway ip-address
```

```
Switch (config-if) # no shutdown
```

工作在第三层的交换机IP地址配置

- 第3层端口的配置
- SVI端口的配置

第3层端口的配置

在默认的情况下,Catalyst2950,3550或4500的每台交换机端口都是第2层接口.当被分配了第3层网络地址并且可以路由选择的时候,交换机的物理端口也可以在第3层接口上进行工作.要使用第3层的功能,必须用下面的命令序列进行配置:

```
Switch(config)# interface type mod/num
```

```
Switch(config-if)# no switchport
```

```
Switch(config-if)# ip address ip-address mask [secondary]
```

no switchport 命令会取消第2层操作的端口.在这之后,必须给该端口分配一个网络地址,也就相当于一个路由器的接口.

SVI端口的配置

使用一个多层交换机的时候,也可以对交换机上的整个VLAN使用第3层功能.这就要求将网络地址分配给一个逻辑接口—VLAN自身的接口.当交换机要为一个公共的VLAN分配许多端口并且需要在这个VLAN内部和外部路由选择的时候,这种方法是非常有效的.

SVI端口的配置

第3层逻辑接口称为SVI.在配置SVI的时候,它需要使用更多的直接接口名称**vlan vlan-id**,好像VLAN自身是一个物理接口.首先,定义或者确定VLAN的接口,然后使用下面的命令为接口分配第3层的所有功能.

```
Switch(config)# interface vlan vlan-id
```

```
Switch(config-if)# ip address ip-address mask  
[secondary]
```

使用SVI之前,VLAN必须在交换机上定义并且将它激活.也要使用**no shutdown** 接口配置命令,确保新的VLAN接口被激活.

交换机的口令安全性配置

通常,网络设备应该配置为对于未被授权的访问是安全的.Catalyst 交换机通常提供一个简单的安全形式,通过设置密码来限制注册到用户接口的人.两种可用的用户访问级别:用户执行模式以及特权模式.用户模式是访问的第一级,.准许访问基本的端口.特权模式需要第二个密码,准许设置或改变交换机操作参数以及配置.

交换机的口令安全性配置

为用户模式设置注册密码,需要在全局配置模式下输入下列命令:

```
Switch (config)# line con 0
```

```
Switch (config-line)# password password
```

```
Switch (config-line)# login
```

```
Switch (config-l)# line vty 0 15
```

```
Switch (config-line)# password password
```

```
Switch (config-line)# login
```

本章小结

本章对交换机原理和基本配置进行了全面的概述。首先，介绍了交换机工作原理与堆叠连接方法；然后，介绍了交换机的主机名配置的命令和交换机IP地址的配置命令；最后，介绍了交换机的口令安全性配置。本章的目的是使读者掌握交换机原理和相关的基本配置。从第6章开始将全面讲述VLAN和相关命令的配置。