

第20章 Catalyst 5000交换机

本章主题

- 局域网交换技术概述
- Catalyst产品线
- Catalyst 交换机上的VLAN配置
- Catalyst 交换机的端口安全配置
- VLAN之间的路由
- Catalyst 交换机故障排除

20.1 引言

本章将讨论Cisco交换机产品，着重Catalyst 5000系列交换机产品。Catalyst 交换机不仅仅是一个快速交换设备，它还支持多个虚拟局域网（VLAN）、先进的路由功能及ATM 局域网仿真。

20.1.1 Catalyst 5000系列概述

Catalyst 5000系列交换机包括四种不同型号，各型号的概要特性如下表所示：

交换机型号	模块化插槽	概要特性
Catalyst 5002	2	支持一个监控模块 可安装一个交换模块
Catalyst 5000	5	支持一个监控模块 可最多安装四个交换模块
Catalyst 5505	5	支持路由交换模块 支持一个监控模块 可安装一个冗余监控模块 可最多安装四个交换模块
Catalyst 5500	13	支持路由交换模块 支持一个监控模块 可安装一个冗余监控模块 可最多安装12个交换模块 支持Lightstream ATM模块 支持路由交换模块

20.1.2 Catalyst 5500产品概述

Catalyst 5500是一个13插槽的高性能交换机，其关键特性包括：

- 3.6Gbps底板。
- 最多达528个交换式10M以太网端口。
- 最多达264个交换式100M以太网端口。

- 最多达132个交换式100M以太网光纤端口。
- 最多达8个ATM OC-12端口。
- 最多达32个DS3 ATM接口。
- 最多达96个25Mbps ATM端口。
- 最多达7个路由交换模块。
- 最多达7个ATM LANE模块。
- 最多达11个FDDI模块。
- 支持双冗余监控引擎能力。
- 热交换模块。
- 热交换电源供应。
- 热交换风扇设备。

20.1.3 Catalyst交换机部件

图20-1列出了Catalyst 5000系列交换机所支持的模块类型。

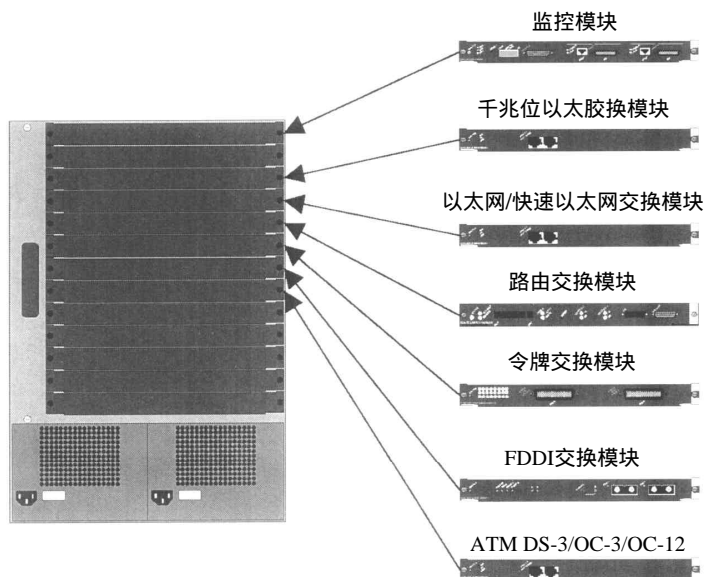


图20-1 Catalyst交换机部件

- 监控引擎 (Supervisor Engine)：监控引擎是Catalyst交换机的主处理器。Catalyst 5500可以安装两块监控引擎，如果其中的一个出现问题，另一个就会代替它工作。II型监控引擎只支持1.2Gbps的背板带宽，III型监控引擎支持3.6Gbps的背板带宽，以及400Mbps的快速以太链接。
- 路由交换模块 (RSM)：该模块为Catalyst交换机提供路由功能。RSM运行普通的Cisco路由器操作系统IOS，在性能上与Cisco 7500路由器相当。RSM没有物理接口，它利用逻辑接口实现不同VLANs之间的路由。
- 以太网/令牌环网/FDDI交换模块：Catalyst交换机支持多种类型的局域网交换，而且还可以由多个100Mbps以太网链路合并为一个逻辑的速率高达800Mbps的全双工快速以太

通道。

20.1.4 虚拟局域网

为了理解虚拟局域网(VLAN)的概念，首先必须了解主机节点连接至局域网的各种方式。

图20-2是一个传统的连接有6台工作站的非交换式以太网，每台工作站与以太网集线器的一个接口相连。一个以太网集线器就是一个独立的冲突域（在任一时刻只能有一台工作站传输数据）和一个独立的广播域（所有的工作站将会接收到另一工作站发送的所有数据流），因此6台工作站处于同一个冲突域和广播域之中。

图20-3所示网络中使用了网桥设备。每3台工作站位于一个局域网中，两个局域网之间通过一个网桥进行连接，与网桥相连的每个局域网是一个单独的冲突域，但所有六台工作站仍属于同一个广播域。

图20-4中采用了路由器设备。每3台工作站位于一个局域网中，两个局域网之间通过一个路由器连接，与路由器相连的每个局域网分别属于单独的冲突域和广播域。

图20-5所示网络中使用的是支持 VLAN 的局域网交换机。所有 6 台工作站连接至同一个 LAN 交换机。

虚拟局域网是在管理上定义的一个广播域，位于同一个 VLAN 中的所有工作站能够接收到该VLAN中某一工作站发送的广播包。听起来 VLAN 与局域网交换差不多，但最关键的区别在于一个VLAN中的所有工作站不受实际物理位置的限制。

该方式中每个VLAN内的3台工作站属于一个单独的广播域，6台工作站分别属于不同的冲突域。

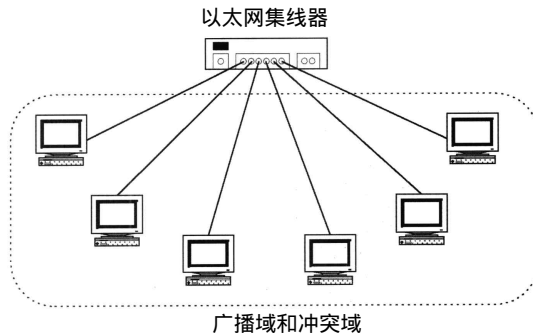


图20-2 以太网集线器

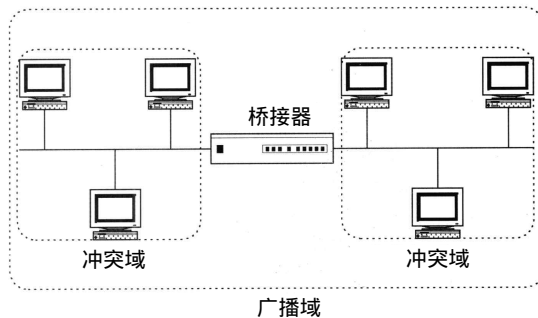


图20-3 网桥示例

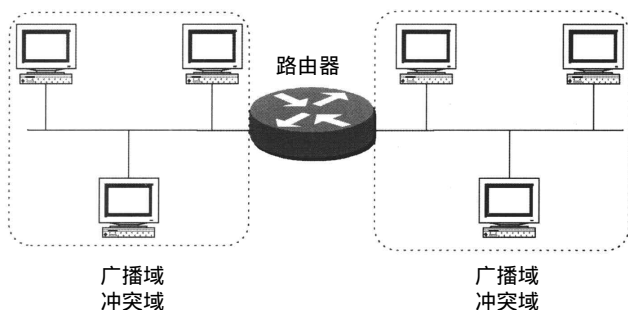


图20-4 路由器连接

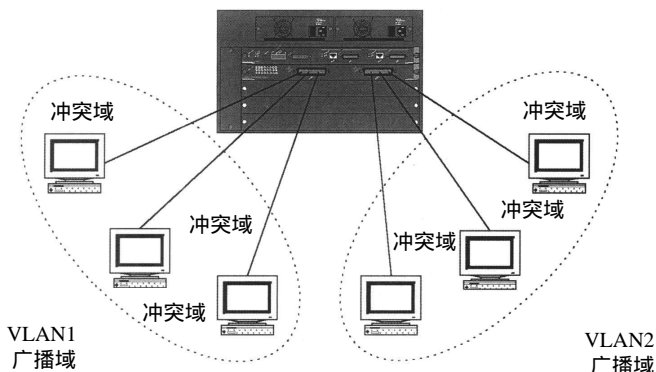


图20-5 局域网交换机连接

20.1.5 VLAN之间的路由

位于两个不同VLAN内的路由器与位于两个不同局域网内的路由器一样，需要考虑如何进行路由的问题。Catalyst交换机可以通过以下两种方式中的一种来实现VLAN之间的路由：

- Catalyst交换机可以采用交换机互连链路（ISL）封装形式通过100Mbps以太网口连接至路由器上。路由器利用子接口（subinterface）来进行VLAN之间的路由，在路由器上为每个VLAN分配不同的子接口号，如图20-6所示。

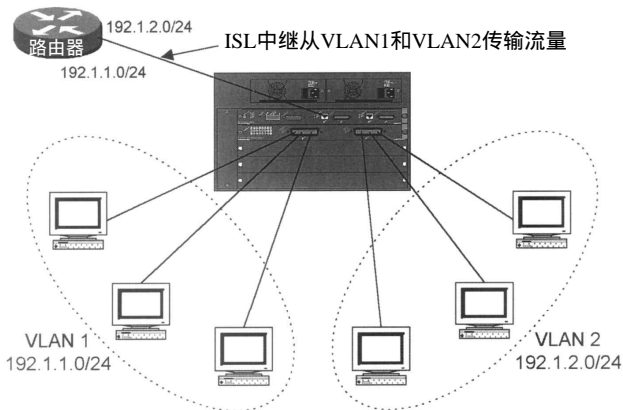


图20-6 VLAN之间的路由

- 使用路由交换模块（RSM）。Catalyst RSM相当于一块卡式的Cisco 7500级别路由器，它没有实际的物理接口，而是使用虚拟接口来实现VLAN之间的路由。

20.1.6 Catalyst交换机的访问

Catalyst 5000系列交换机拥有一个被称为SC0的内部逻辑接口，SC0接口提供一个有效的IP地址用于远程登录（telnet）到交换机上进行配置和监测，通常该接口位于VLAN1，但也可被移动到其他VLAN中。如果没有SC0接口，对交换机的访问必须通过监控模块上的控制口或者Aux端口。Catalyst交换机还支持SLIP连接，配置SLIP IP地址时只需在交换机的SL0接口上定义即可。

20.1.7 Catalyst交换机中继

Catalyst交换机的用户端口也可以定义为中继口，用于Catalyst交换机之间的连接和交换机与路由器的连接。

20.1.8 Catalyst交换机配置

Catalyst交换机的配置与Cisco路由器的配置有些不同，表现在以下几个方面：

- 路由器有一个专门的配置模式，而在Catalyst交换机中，则直接在特权模式的命令行提示符状态下输入命令。但两者都是在配置作出修改后立即生效。
- 路由器有几种运行模式，如执行模式、调试模式和配置模式等等，而Catalyst交换机只有用户模式和特权模式两种。
- 路由器的配置有两种存储方式：当前运行配置和开机启动配置。当前运行配置是目前路由器中处于工作状态的配置，而开机启动配置则是保存在NVRAM中的配置。当对路由器的配置进行修改时，当前运行配置随着发生变化，但开机启动配置并不改变。在Catalyst交换机中，配置只有一种存储方式，对交换机配置作出的任何修改都将保存下来。
- 在路由器中show run命令将显示当前运行配置，路由器的配置通常比较短，只列出输入的配置命令和非缺省的命令项。Catalyst交换机的配置比较长，它列出该交换机的每一个参数，而不管这些参数是不是用户所配置的。以下为从交换机配置中摘录的部分内容。

```
#module 5 : 12-port 10/100BaseTX Ethernet
set module name      5
set module enable    5
set VLAN 1           5/1-10
set VLAN 2           5/11-12
set port channel 5/1-12 off
set port channel 5/1-12 auto
set port enable      5/1-12
set port level       5/1-12 normal
set port speed       5/1-12 auto
set port trap        5/1-12 disable
set port name        5/11 RouterB
set port name        5/12 RouterA
set port name        5/1-10
set port security    5/1-12 disable
set port broadcast   5/1-12 0
set port membership  5/1-12 static
```

```

set cdp enable 5/1-12
set cdp interval 5/1-12 60
set trunk 5/1 auto 1-1005
set trunk 5/2 auto 1-1005
set trunk 5/3 auto 1-1005
set trunk 5/4 auto 1-1005
set trunk 5/5 auto 1-1005
set trunk 5/6 auto 1-1005
set trunk 5/7 auto 1-1005
set trunk 5/8 auto 1-1005
set trunk 5/9 auto 1-1005
set trunk 5/10 auto 1-1005
set trunk 5/11 auto 1-1005
set trunk 5/12 off 1-1005
set spantree portfast 5/1-12 disable
set spantree portcost 5/1 100
set spantree portcost 5/2 100
set spantree portcost 5/3 100
set spantree portcost 5/4 100
set spantree portcost 5/5 100
set spantree portcost 5/6 100
set spantree portcost 5/7 100
set spantree portcost 5/8 100
set spantree portcost 5/9 100
set spantree portcost 5/10 100
set spantree portcost 5/11 100
set spantree portcost 5/12 100
set spantree portpri 5/1-12 32
set spantree portvlanpri 5/1 0
set spantree portvlanpri 5/2 0
set spantree portvlanpri 5/3 0
set spantree portvlanpri 5/4 0
set spantree portvlanpri 5/5 0
set spantree portvlanpri 5/6 0
set spantree portvlanpri 5/7 0
set spantree portvlanpri 5/8 0
set spantree portvlanpri 5/9 0
set spantree portvlanpri 5/10 0
set spantree portvlanpri 5/11 0
set spantree portvlanpri 5/12 0
set spantree portvlancost 5/1 cost 99
set spantree portvlancost 5/2 cost 99
set spantree portvlancost 5/3 cost 99
set spantree portvlancost 5/4 cost 99
set spantree portvlancost 5/5 cost 99
set spantree portvlancost 5/6 cost 99
set spantree portvlancost 5/7 cost 99
set spantree portvlancost 5/8 cost 99
set spantree portvlancost 5/9 cost 99
set spantree portvlancost 5/10 cost 99
set spantree portvlancost 5/11 cost 99
set spantree portvlancost 5/12 cost 99

```

20.2 本章所讨论的命令

- **clear config all**
- **ping host** *[packet_size] [packet_count]*
- **set interface sc0** *[ip_addr [netmask [broadcast]]]*
- **set ip permit {enable | disable} / set ip permit** *ip_addr [mask]*
- **set port name** *mod_num / port_num [name_string]*
- **set port security** *mod_num / port_num {enable | disable} [mac_addr]*

- **set trunk** *mod_num/port_num* [on | off | desirable | auto]
[*vlan_range*]
- **set vlan** *vlan_num mod_num/port_num*
- **set vtp domain** *name*
- **show cam dynamic**
- **show interface**
- **show ip permit**
- **show mac** [*mod_num/[port_num]*]
- **show module** *mod_num*
- **show port** [*mod_num/port_num*]
- **show system**
- **show trunk** [*mod_num[/port_num]*]
- **show version**
- **show vlan** [*vlan*]
- **show vtp domain**

命令的定义

- clear config all: 该特权命令清除 Catalyst 交换机的所有配置，重新设置交换机。
- ping: 这是一个用户模式命令，它向选定节点发送 ICMP 回波请求。
- set interface: 该特权命令可设置用于带内 telnet 和进行 SNMP 访问的 SC0 接口，也可设置用于 SLIP 远程登录和进行 SNMP 访问的 SL0 接口。
- set ip permit: 该特权命令激活或者取消 IP 访问列表，在 IP 访问列表中创建一项列表。
- set port name: 该特权命令用于设置 Catalyst 交换机的端口名。
- set port security: 该特权命令用于激活或取消交换机 MAC 级的端口安全设置。
- set trunk: 该特权命令将 Catalyst 交换机的端口设置为中继端口。
- set vlan: 该特权命令用于配置交换机中的 VLAN。
- set vtp domain: 该特权命令设置 VTP 域名。
- show cam dynamic: 该命令是一个用户模式命令，它显示 CAM 表的内容。
- show interface: 该命令用于显示 Catalyst 交换机的接口信息。
- show ip permit: 该命令可显示 Catalyst 交换机上配置的 IP 访问列表信息。
- show mac: 该命令显示关于交换机的 MAC 级的统计信息。
- show module: 该命令给出 Catalyst 交换机的模块信息。
- show port: 该命令给出关于交换机的端口级的统计信息。
- show system: 该命令用于显示 Catalyst 交换机的系统信息。
- show trunk: 该命令提供交换机的中继信息。
- show version: 该命令用于显示交换机的硬件和软件版本信息。
- show vlan: 该命令显示交换机的 VLAN 信息。
- show vtp domain: 该命令用于显示交换机的 VTP 域信息。

20.3 IOS 需求

本章实验中使用的是 IOS 11.2 版。IOS 11.2 版及更高版本支持 ISL 中继。Catalyst 交换机中

运行的是3.1版操作系统。

20.4 实验77：基本Catalyst交换机配置、VLAN和端口安全设置

20.4.1 所需设备

为完成本实验需要下列设备：

- 1) 带以太网口的两台路由器；
- 2) 带10Mbps或100Mbps以太网端口的Catalyst交换机；
- 3) 两根以太网电缆；
- 4) Cisco路由器控制口电缆；
- 5) 连接路由器控制口和Catalyst交换机的直连电缆。

20.4.2 配置概述

本实验将演示如何配置用于简单局域网交换的 Catalyst 5500交换机。两台路由器（路由器A和路由器B）与Catalyst交换机的连接方式如图20-7所示，这两台路由器将属于同一个VLAN，Catalyst交换机上将设置两种安全特性：IP许可和MAC过滤。

- IP许可：该特性允许最多达 10个IP地址进入 Catalyst交换机，而且该交换机只接受来自预定义的这10个IP地址的远程登录和SNMP数据包。如果其他未经授权的地址试图向交换机发送远程登录和SNMP数据包，交换机将予以拒绝，并且记录该被拒绝的IP地址。
- MAC过滤：可以配置Catalyst交换机的某端口使它拒绝来自在交换机中未预定义的MAC地址的数据流。

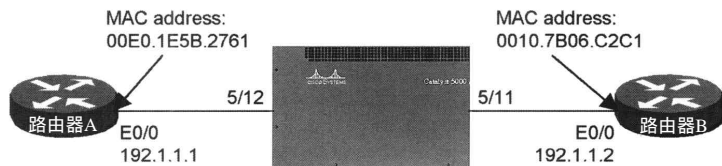


图20-7 具有端口安全特性的交换机配置

注意 Cisco生产许多型号的局域网交换机，本实验中使用的是Catalyst 5500交换机，也可以用其它一些Cisco交换机设备来完成，如装有企业级版软件的Catalyst 1924交换机就是一款较便宜的交换机设备，它同样支持VLAN和100Mbps ISL中继。

Catalyst交换机与Cisco路由器使用的IOS操作系统不同，命令设置方式也不一样。许多在路由器中具有的特性，如使用Tab键来结束一条命令的输入，不能想当然地用于Catalyst交换机。另外，Catalyst交换机中的端口是通过插槽号和端口号来确定的，如本实验中两台路由器分别与第5槽的第11和第12端口连接，在Catalyst交换机中分别被表示为5/11和5/12。

20.4.3 路由器配置

本实验中两台路由器的配置情况如下所示：

1. 路由器A

```

Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname RouterA
!
interface Ethernet0/0
  ip address 192.1.1.1 255.255.255.0←Define the IP address for the interface
                                   connected to the Catalyst switch
!
no ip classless
!
line con 0
line aux 0
line vty 0 4
  exec-timeout 30 0
  login
!
end

```

2. 路由器B

```

Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname RouterB
!
interface Ethernet0/0
  ip address 192.1.1.2 255.255.255.0←Define the IP address for the interface
                                   connected to the Catalyst switch
!
no ip classless
!
line con 0
line aux 0
line vty 0 4
  exec-timeout 30 0
  login
!
end

```

20.4.4 监测配置

连接Catalyst 5500交换机。首先我们从清除它所有的配置开始，运行 clear config all命令使交换机回到厂家默认配置状态。

```

Console> (enable) clear config all
This command will clear all configuration in NVRAM.
This command will cause ifIndex to be reassigned on the next system startup.
Do you want to continue (y/n) [n]? y
.....
.....
.....
.....
.....
System configuration cleared.

```

在Catalyst交换机重新启动后，所有端口都被定义为同一个 VLAN：VLAN1。这时的Catalyst是一个多端口的局域网交换机，它将自动检测与其端口相连的局域网并正确地设置相应端口的参数。可以用show port命令看到端口5/11和5/12已被自动配置，它们的状态为“已连接”，都属于VLAN 1，运行的是10Mbps速率的半双工以太网。注意我们在使交换机回到厂家默认配置状态重启之后无需手工配置5/11和5/12端口。

```
Console> (enable) sh port
Port  Name      Status      Vlan      Level      Duplex      Speed      Type
-----
5/11      connected    1          normal     a-half     a-10       10/100BaseTX
5/12      connected    1          normal     a-half     a-10       10/100BaseTX
```

关于端口的更详细的信息可以通过在show port命令后加端口号得到。输入show port 5/11命令，可以看到关于端口5/11的附加信息，包括MAC级安全信息，以太网冲突和错误信息等。

```
Console> (enable) sh port 5/11
Port  Name      Status      Vlan      Level      Duplex      Speed      Type
-----
5/11      connected    1          normal     a-half     a-10       10/100BaseTX
Port      Security    Secure-Src-Addr  Last-Src-Addr  Shutdown      Trap
-----
5/11      disabled
No disabled

Port  Broadcast-Limit  Broadcast-Drop
-----
5/11      -                0
Port      Status      Channel  Channel      Neighbor      Neighbor
-----
5/11      connected    auto     not channel
-----

Port      Align-Err  FCS-Err  Xmit-Err  Rcv-Err  UnderSize
-----
5/11      0          0        0         0        0
-----

Port      Single-Col  Multi-Coll  Late-Coll  Excess-Col  Carri-Sen  Runts  Giants
-----
5/11      0          0          0         0          0          0      0
-----

Last-Time-Cleared
-----
Sun May 16 1999, 02:25:04
```

可以设置交换机端口的名称以便更容易地区分，用set port name命令来为端口5/11和5/12命名。

```
Console> (enable) set port name 5/11 RouterB
Port 5/11 name set.
Console> (enable) set port name 5/12 RouterA
Port 5/12 name set.
```

现在执行show port 5/12命令，可以看到端口5/12已被设置为“RouterA”。

```
Console> (enable) sh port 5/12
Port  Name      Status      Vlan      Level      Duplex      Speed      Type
-----
5/12      RouterA    connected    1          normal     a-half     a-10       10/100BaseTX
Port      Security    Secure-Src-Addr  Last-Src-Addr  Shutdown      Trap
-----
5/12      disabled
No disabled

Port  Broadcast-Limit  Broadcast-Drop
-----
```

5/12	-	0						
Port	Status	Channel mode	Channel status	Neighbor device	Neighbor port			
5/12	connected	auto	not channel					
Port	Align-Err	FCS-Err	Xmit-Err	Rcv-Err	UnderSize			
5/12	0	0	0	0	0			
Port	Single-Col	Multi-Coll	Late-Coll	Excess-Col	Carri-Sen	Runts	Giants	
5/12	0	0	0	0	0	0	0	

Last-Time-Cleared

Sun May 16 1999, 02:25:04

连接至路由器 B，证实从路由器 B 可以 ping 通路由器 A 的 IP 地址为 192.1.1.1 的接口。注意路由器 A 和 B 在交换机重启时被自动置于 VLAN 1。

```
RouterB#ping 192.1.1.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.1.1.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Catalyst 交换机可分配一个用于 Telnet 和 SNMP 访问的内部 IP 地址，可以用 show interface 命令来查看该内部 IP 地址。下面的显示中，交换机没有设置 IP 地址。

```
Console> (enable) sh interface
```

```
sl0: flags=51<UP, POINTOPOINT, RUNNING>
```

```
slip 0.0.0.0 dest 128.73.35.160
```

```
sc0: flags=63<UP, BROADCAST, RUNNING>
```

```
VLAN 1 inet 0.0.0.0 netmask 0.0.0.0 broadcast 0.0.0.0
```

用于带内访问用途的 IP 地址可以通过 set interface sc0 命令在交换机上设置。下例中为 sc0 配置 IP 地址 192.1.1.3，注意该地址与路由器 A 的以太网口地址（192.1.1.1）和路由器 B 的以太网口地址（192.1.1.2）位于同一个网络。

```
Console> (enable) set interface sc0 192.1.1.3
```

```
Interface sc0 IP address set.
```

这时执行 show interface 命令将显示 sc0 的 IP 地址已被设为 192.1.1.3。

```
Console> (enable) sh interface
```

```
sl0: flags=51<UP, POINTOPOINT, RUNNING>
```

```
slip 0.0.0.0 dest 128.73.35.160
```

```
sc0: flags=63<UP, BROADCAST, RUNNING>
```

```
VLAN 1 inet 192.1.1.3 netmask 255.255.255.0 broadcast 192.1.1.255
```

设定 sc0 的 IP 地址后，就可以直接 ping 该地址确认其为激活状态。

```
Console> (enable) ping 192.1.1.3
```

```
192.1.1.3 is alive
```

我们还可以 ping 路由器 A 和路由器 B。

```
Console> (enable) ping 192.1.1.1
```

```
192.1.1.1 is alive
```

```
Console> (enable) ping 192.1.1.2
```

```
192.1.1.2 is alive
```

路由器 A 和路由器 B 都应当可以 ping 通 Catalyst 交换机的 sc0 接口。下面证实从路由器 A 可以 ping 通 Catalyst 交换机。

```
RouterA#ping 192.1.1.3
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.1.1.3, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

20.4.5 IP许可列表

Catalyst交换机提供了强大的安全特性，其中一个就是交换机的IP列表访问能力。Catalyst交换机的IP访问特性允许用户定义最多达10个IP地址对交换机进行SNMP访问和远程登录。访问列表可以用命令show ip permit进行查询，下面的显示说明交换机的访问列表中尚未定义IP地址。

```
Console> (enable) show ip permit
```

```
IP permit list feature disabled.
```

```
Permit List      Mask
```

```
-----
```

```
Denied IP Address      Last Accessed Time      Type
```

```
-----
```

可以用命令set ip permit 192.1.1.1在交换机的访问列表中增加一个IP地址，该命令将允许路由器A对Catalyst交换机进行远程登录或SNMP访问。

```
Console> (enable) set ip permit 192.1.1.1
```

```
192.1.1.1 added to IP permit list.
```

这时用show ip permit命令可以看到192.1.1.1已经在访问列表中了，注意IP访问列表特性当前处于关闭状态，这是访问列表的缺省状态。

```
Console> (enable) show ip permit
```

```
IP permit list feature disabled.
```

```
Permit List      Mask
```

```
-----
```

```
192.1.1.1
```

```
Denied IP Address      Last Accessed Time      Type
```

```
-----
```

在定义了IP访问列表之后，必须用set ip permit enable命令将其激活。

```
Console> (enable) set ip permit enable
```

```
IP permit list enabled.
```

现在再连接至路由器B，它与Catalyst交换机相连的以太网口的IP地址为192.1.1.2，该地址不在交换机的IP访问列表中。在路由器B上ping交换机的SC0接口，结果能够ping通。需要引起注意的是，IP访问列表只是拒绝其他IP地址对交换机的SNMP和远程登录访问。

```
RouterB#ping 192.1.1.3
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.1.1.3, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

在路由器B上尝试远程登录到Catalyst交换机的IP地址192.1.1.3，将看到交换机拒绝了远程登录会话，因为路由器B的以太网口地址192.1.1.2并不在交换机的IP访问列表中。

```
RouterB#telnet 192.1.1.3
```

```
Trying 192.1.1.3 ... Open
```

```
Access not permitted. Closing connection...
```

```
[Connection to 192.1.1.3 closed by foreign host]
```

我们再连接至 Catalyst 交换机，用 show ip permit 命令查看 IP 访问列表，可以发现交换机记录了刚才所做的远程登录尝试，记录中包括被拒绝的 IP 地址及其活动。

```
Console> (enable) show ip permit
IP permit list feature enabled.
Permit List      Mask
-----
192.1.1.1

Denied IP Address      Last Accessed Time      Type
-----
192.1.1.2              05/25/99,14:25:50      Telnet
```

可以用 set ip permit disable 命令取消 IP 访问列表。

```
Console> (enable) set ip permit disable
IP permit list disabled.
```

重新连接至路由器 B 并尝试远程登录到交换机上，将发现远程登录成功，这是因为 IP 访问列表已经被取消。

```
RouterB#telnet 192.1.1.3
Trying 192.1.1.3 ... Open

Cisco Systems Console

Enter password:
Console> ena
Enter password:
Console> (enable)
Console> (enable) exit

[Connection to 192.1.1.3 closed by foreign host]
```

20.4.6 安全端口过滤

可以对 Catalyst 交换机进行配置，使得它的某端口只接收来自预定义的 MAC 地址的数据流，这一特性被称为安全端口过滤。从下面 show port 5/12 命令的输出可以看到该端口的 MAC 源地址项为空。

```
Console> (enable) sh port 5/12
Port  Name      Status      Vlan      Level      Duplex      Speed      Type
-----
5/12  RouterA  connected   1         normal     a-half     a-10      10/100BaseTX

Port      Security      Secure-Src-Addr      Last-Src-Addr      Shutdown      Trap
-----
5/12      disabled

Port      Broadcast-Limit      Broadcast-Drop
-----
5/12      -                    0

Port      Status      Channel mode      Channel status      Neighbor device      Neighbor port
-----
5/12      connected   auto              not channel

Port      Align-Err      FCS-Err      Xmit-Err      Rcv-Err      UnderSize
-----
5/12      0              0              0              0              0

Port      Single-Col      Multi-Coll      Late-Coll      Excess-Col      Carri-Sen      Runts      Giants
-----
5/12      0              0              0              0              0              0              0
```

Last-Time-Cleared

Sun May 16 1999, 02:25:04

下面设置端口 5/12，使它只接收来自特定 MAC 地址的数据流。为了配置 Catalyst 交换机的安全端口过滤，首先必须知道与端口 5/12 相连的主机的 MAC 地址。本实验中，与 Catalyst 交换机的端口 5/12 相连的是路由器 A 的以太网接口 e0/0。连接至路由器 A，执行 show interface e0/0 命令查看以太网口 e0/0 的 MAC 地址，得知其 MAC 地址为 00e0.1e5b.2761。

```
RouterA#sh int e 0/0
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is 00e0.1e5b.2761 (bia 00e0.1e5b.2761)
  Internet address is 192.1.1.1/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:22, output 00:00:07, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    18672 packets input, 17647218 bytes, 0 no buffer
    Received 3662 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    24112 packets output, 18236637 bytes, 0 underruns
    118 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 1 deferred
    118 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

现在与 Catalyst 交换机相连，用如下所示的 set port security 命令定义交换机端口 5/12 所接受的 MAC 地址。

```
Console> (enable) set port security 5/12 enable 00-e0-1e-5b-27-62
Port 5/12 port security enabled with 00-e0-1e-5b-27-62 as the secure mac address
Trunking disabled for Port 5/12 due to Security Mode
```

这时在路由器 A 上试图 ping 交换机的 sc0 接口 IP 地址 192.1.1.3，结果不成功。

```
RouterA#ping 192.1.1.3
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.1.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

连接至 Catalyst 交换机可以发现端口 5/12 处于关闭状态，该端口被关闭的原因可从 Secure-Src-Addr 和 Last-Src-Addr 两栏得到解释。这两栏列出了来自哪些 MAC 地址的数据被允许进入交换机端口以及最后一个向端口发送数据的 MAC 地址。在下面的输出中可以看到 Secure-Src-Addr 和 Last-Src-Addr 两栏中的内容不相匹配。

```
Console> (enable) show port 5/12
```

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
5/12	RouterA	shutdown	1	normal	a-half	a-10	10/100BaseTX

Port	Security	Secure-Src-Addr	Last-Src-Addr	Shutdown	Trap
5/12	enabled	00-e0-1e-5b-27-62	00-e0-1e-5b-27-61	Yes	Disabled

Port	Broadcast-Limit	Broadcast-Drop
------	-----------------	----------------

```

-----
5/12 - 0
Port Status Channel mode Channel status Neighbor device Neighbor port
-----
5/12 shutdown auto not channel
Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize
-----
5/12 0 0 0 0 0

Port Single-Col Multi-Coll Late-Coll Excess-Col Carri-Sen Runts Giants
-----
5/12 0 0 0 0 0 0 0

```

Last-Time-Cleared

Sun May 16 1999, 02:25:04

用set port security 5/12 disable命令可以取消在端口5/12所作的设置。

```

Console> (enable) set port security 5/12 disable
Port 5/12 port security disabled.

```

执行命令show port 5/12查看端口状态，可以发现该端口的状态变为连接状态。

```

Console> (enable) sh port 5/12
Port Name Status Vlan Level Duplex Speed Type
-----
5/12 RouterA connected 1 normal a-half a-10 10/100BaseTX

Port Security Secure-Src-Addr Last-Src-Addr Shutdown Trap
-----
5/12 disabled No disabled

Port Broadcast-Limit Broadcast-Drop
-----
5/12 - 0
Port Status Channel mode Channel status Neighbor device Neighbor port
-----
5/12 connected auto not channel

Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize
-----
5/12 0 0 0 0 0

Port Single-Col Multi-Coll Late-Coll Excess-Col Carri-Sen Runts Giants
-----
5/12 0 0 0 0 0 0 0

Last-Time-Cleared
-----
Sun May 16 1999, 02:25:04

```

这时在路由器A上又可以ping通路由器B的接口IP地址192.1.1.2。

```

RouterA#ping 192.1.1.2

```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.1.1.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms

下面将把路由器A和路由器B移到VLAN 2。前面讲过，当Catalyst交换机清除配置重新启动时，它把所有端口设置在VLAN 1中。在设置其他VLAN号以前，Catalyst交换机必须拥有一个域名。下面show vtp domain命令的输出说明交换机还没有设置域名。


```
Console> (enable) sh vtp domain
```

Domain Name	Domain Index	VTP Version	Local Mode	Password
	1	2	server	-

Vlan-count	Max-vlan-storage	Config Revision	Notifications
5	1023	0	disabled

Last Updated	V2 Mode	Pruning	PruneEligible on Vlans
0.0.0.0	disabled	disabled	2-1000

用命令set vtp domain CCIE_STUDY_GUIDE为交换机设置一个域名。

```
Console> (enable) set vtp domain CCIE_STUDY_GUIDE
VTP domain CCIE_STUDY_GUIDE modified
```

```
Console> (enable) show vtp domain
```

Domain Name	Domain Index	VTP Version	Local Mode	Password
CCIE_STUDY_GUIDE	1	2	server	-

Vlan-count	Max-vlan-storage	Config Revision	Notifications
5	1023	0	disabled

Last Updated	V2 Mode	Pruning	PruneEligible on Vlans
0.0.0.0	disabled	disabled	2-1000

使用set VLAN 2 5/11命令将端口5/11移到VLAN 2，注意交换机会自动修改VLAN 1，将端口5/11从VLAN 1中移去。

```
Console> (enable) set VLAN 2 5/11
VLAN 2 configuration successful
VLAN 2 modified.
VLAN 1 modified.
VLAN Mod/Ports
-----
2      5/11
```

同样，使用set VLAN 2 5/12命令将端口5/12移到VLAN 2。

```
Console> (enable) set VLAN 2 5/12
VLAN 2 modified.
VLAN 1 modified.
VLAN Mod/Ports
-----
2      5/11-12
```

用命令set VLAN 2激活该虚拟局域网。

```
Console> (enable) set VLAN 2
VLAN 2 configuration successful
```

这时show VLAN 2命令将显示VLAN 2处于激活状态，包含两个端口：5/11和5/12。

```
Console> (enable) sh VLAN 2
```

VLAN Name	Status	Mod/Ports, Vlans
2 VLAN0002	active	5/11-12

VLAN	Type	SAID	MTU	Parent	RingNo	BrdgNo	Stp	BrdgMode	Trans1	Trans2
2	enet	100002	1500	-	-	-	-	-	0	0

VLAN	AREHops	STEHops	Backup CRF
-----	-----	-----	-----

VLAN的状态也可以通过命令 show vlan来得知，从下面的显示可以看出交换机的其他以太网端口仍然位于缺省的VLAN 1中。

Console> (enable) sh vlan		
VLAN Name	Status	Mod/Ports, Vlans
-----	-----	-----
1 default	active	2/1-2
		3/1-24
		5/1-10
		7/1-24
		10/1-24
2 VLAN0002	active	5/11-12
1002 fddi-default	active	
1003 token-ring-default	active	12/1-16
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BrdgNo	Stp	BrdgMode	Trans1	Trans2
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
1	enet	100001	1500	-	-	-	-	-	0	0
2	enet	100002	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	0x0	-	-	-	0	0
1003	trcrf	101003	1500	0	0x0	-	-	-	0	0
1004	fdnet	101004	1500	-	-	0x0	ieee	-	0	0
1005	trbrf	101005	1500	-	-	0x0	ibm	-	0	0

VLAN	AREHops	STEHops	Backup CRF
-----	-----	-----	-----
1003	7	7	off

可以通过从路由器 A上ping路由器B的IP地址 192.1.1.2来证实VLAN 2处于正常工作状态。下面显示能够ping通，所以路由器 A和B都属于VLAN 2。

```
RouterA#ping 192.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.1.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms
```

20.5 实验78：用ISL中继实现VLAN之间的路由

20.5.1 所需设备

- 为完成本实验需要下列设备：
- 1) 带以太网口的两台 Cisco路由器；
 - 2) 带100Mbps以太网口的Cisco路由器一台；
 - 3) Catalyst交换机一台；
 - 4) 三根以太网网线；
 - 5) Cisco路由器控制口电缆；
 - 6) 连接路由器控制口和Catalyst交换机的直连电缆。

[illegible]

```
router rip
 network 192.1.1.0
!
no ip classless
!
line con 0
line aux 0
line vty 0 4
 exec-timeout 30 0
 login
!
end
```

2. 路由器B

Current configuration:

```
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname RouterB
!
!
!
interface Ethernet0/0
 ip address 193.1.1.1 255.255.255.0←Define the IP address for the interface
 connected to the Catalyst switch
!
router rip
 network 193.1.1.0
!
no ip classless
!
line con 0
line aux 0
line vty 0 4
 exec-timeout 30 0
 login
!
end
```

3. 路由器C

Current configuration:

```
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname RouterC
!
interface FastEthernet1/0←This 100Mb/s interface connects to the Catalyst
 trunk port
 no ip address
 no logging event subif-link-status
!
interface FastEthernet1/0.1←This subinterface accepts traffic from VLAN 1
 encapsulation isl 1←Define ISL encapsulation and accept traffic from VLAN 1
 ip address 192.1.1.10 255.255.255.0←IP address for this subinterface
 no ip redirects
!
interface FastEthernet1/0.2←This subinterface accepts traffic from VLAN 2
 encapsulation isl 2←Define ISL encapsulation and accept traffic from VLAN 2
 ip address 193.1.1.10 255.255.255.0←IP address for this subinterface
 no ip redirects
```

```

!
router rip←We need to dynamically route between VLAN 1 and VLAN 2. Our routes
        will be learned via RIP
  network 192.1.1.0←Propagate RIP for the network on VLAN 1
  network 193.1.1.0←Propagate RIP for the network on VLAN 2
!
no ip classless
!
!
line con 0
line aux 0
line vty 0 4
  login
!
end

```

20.5.4 监测配置

首先用clear config all命令使Catalyst 5500交换机清除它所有的配置，回到厂家默认配置状态，从前面的实验中得知，在交换机重新启动之后，它所有的以太网端口属于 VLAN 1。

```

Console> (enable) clear config all
This command will clear all configuration in NVRAM.
This command will cause ifIndex to be reassigned on the next system startup.
Do you want to continue (y/n) [n]? y
.....
.....
.....
.....
.....
.....

```

System configuration cleared.

因为要将交换机的端口划分到多个 VLAN 中，必须先用set vtp domain命令设置Catalyst交换机的VTP域名。

```

Console> (enable) set vtp domain CCIE_LAB
VTP domain CCIE_LAB modified

```

端口5/12位于VLAN 1，无需通过命令来设置该端口，因为 VLAN 1是交换机端口的默认值。必须用set VLAN 2 5/11命令将端口5/11划分到VLAN 2中。

```

Console> (enable) set VLAN 2 5/11
VLAN 2 configuration successful
VLAN 2 modified.
VLAN 1 modified.
VLAN    Mod/Ports
----    -
2       5/10-11

```

然后用命令set VLAN 2激活该VLAN2。

```

Console> (enable) set VLAN 2
VLAN 2 configuration successful

```

实验中以端口5/10作为中继端口，它与Cisco路由器相连，将所有VLAN的数据流传输到路由器，路由器就可以在不同VLAN之间进行路由。使用命令set trunk 5/10 on将端口5/10设为中继模式。

```

Console> (enable) set trunk 5/10 on
Port(s) 5/10 trunk mode set to on.

```

端口5/10的状态可以由命令show port 5/10来查看，可以看到该端口处于激活状态并被设

置为中继端口，工作方式为 100Mbps 全双工方式。

```

Console> (enable) sh port 5/10
Port   Name      Status      Vlan    Level    Duplex    Speed    Type
-----
5/10   -         connected   trunk   normal   a-full    a-100    10/100BaseTX

Port   Security  Secure-Src-Addr  Last-Src-Addr  Shutdown  Trap
-----
5/10   disabled

Port   Broadcast-Limit  Broadcast-Drop
-----
5/10   -                -

Port   Status      Channel mode  Channel status  Neighbor device  Neighbor port
-----
5/10   connected   auto         not channel

Port   Align-Err  FCS-Err  Xmit-Err  Rcv-Err  UnderSize
-----
5/10   0          0        0         0        0

Port   Single-Col  Multi-Coll  Late-Coll  Excess-Col  Carri-Sen  Runts  Giants
-----
5/10   0          0          0         0          0          0      -

Last-Time-Cleared
-----
Sun May 16 1999, 02:25:04

```

可以证实路由器 A 和路由器 B 是连通的，注意端口 5/11（路由器 B）位于 VLAN 2，而端口 5/12（路由器 A）位于 VLAN 1。

```

Console> (enable) sh port 5/11
Port   Name      Status      Vlan    Level    Duplex    Speed    Type
-----
5/11   -         connected   2       normal   a-half    a-10     10/100BaseTX

Console> (enable) sh port 5/12
Port   Name      Status      Vlan    Level    Duplex    Speed    Type
-----
5/12   -         connected   1       normal   a-half    a-10     10/100BaseTX

```

show trunk 命令给出有关中继的具体信息，包括该中继上哪些 VLAN 是可以进入的，哪些 VLAN 当前处于激活状态。本实验中，中继端口 5/10 允许来自所有 VLAN 的数据流进入。

```

Console> (enable) sh trunk
Port   Mode      Status
-----
5/10   on        trunking

Port   Vlans allowed on trunk
-----
5/10   1-1005

Port   Vlans allowed and active in management domain
-----
5/10   1-2,1003,1005

Port   Vlans in spanning tree forwarding state and not pruned
-----
5/10   1-2,1003,1005

```

现在在路由器 A 上用 show ip route 命令来显示其路由表，可以看到存在一条到网络 193.1.1.0 的路由。路由器 B 与 Catalyst 交换机连接的网络 193.1.1.0 属于 VLAN 2。从路由器 A 的路由表可以说明路由器 C 工作正常，并在两个 VLAN 之间提供路由。

```
RouterA#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
        U - per-user static route, o - ODR
```

Gateway of last resort is not set

```
C    192.1.1.0/24 is directly connected, Ethernet0/0
R    193.1.1.0/24 [120/1] via 192.1.1.10, 00:00:26, Ethernet0/0
```

端到端的连通性可以通过在路由器 A 上 ping IP 地址 193.1.1.1 来验证，可以看到结果是成功的。

```
RouterA#ping 193.1.1.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 193.1.1.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

在路由器 B 上用 show ip router 命令显示其路由表，可以看到它通过 RIP 路由协议发现了通往路由器 A 的路由。

```
RouterB#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
        U - per-user static route, o - ODR
```

Gateway of last resort is not set

```
R    192.1.1.0/24 [120/1] via 193.1.1.10, 00:00:10, Ethernet0/0
C    193.1.1.0/24 is directly connected, Ethernet0/0
```

在路由器 B 上可以 ping 通路由器 A 的 IP 地址为 192.1.1.1 的接口。

```
RouterB#ping 192.1.1.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.1.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
```

现在连接至路由器 C，用 show ip route 命令查看其路由表，可以看到路由器 C 有两个直接相连的网络，这两个网络都由同一个 100Mbps 以太网物理接口进入该路由器。路由器 C 的 100Mbps 以太网口上定义了两个子接口，VLAN 1 与子接口 FastEthernet1/0.1 相连，而 VLAN 2 与子接口 FastEthernet1/0.2 相连。

```
RouterC#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
        U - per-user static route, o - ODR
```


Gateway of last resort is not set

C 192.1.1.0/24 is directly connected, **FastEthernet1/0.1**
C 193.1.1.0/24 is directly connected, **FastEthernet1/0.2**

从路由器C可以ping通路由器A和B，这说明中继链路工作正常。

RouterC#ping 192.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.1.1.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

RouterC#ping 193.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 193.1.1.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

20.6 故障查找

show version 该命令用于显示关于交换机的重要的系统级信息，包括硬件版本、交换机中各模块的序列号、系统内存和系统已运行时间。

```
Console> (enable) show ver
WS-C5500 Software, Version MpsSW: 3.1(1) NmpSW: 3.1(1)
Copyright (c) 1995-1997 by Cisco Systems
NMP S/W compiled on Dec 31 1997, 18:36:38
MCP S/W compiled on Dec 31 1997, 18:33:15
```

System Bootstrap Version: 3.1(2)

Hardware Version: 1.3 Model: WS-C5500 Serial #: 069028115

Module	Ports	Model	Serial #	Hw	Fw	Fw1	Sw
2	2	WS-X5530	008167898	1.8	3.1(2)	4.1(1)	3.1(1)
3	24	WS-X5224	008161402	1.3	3.1(1)		3.1(1)
5	12	WS-X5203	008451509	1.1	3.1(1)		3.1(1)
7	24	WS-X5224	008161009	1.3	3.1(1)		3.1(1)
10	24	WS-X5224	008161288	1.3	3.1(1)		3.1(1)
12	16	WS-X5030	007380744	1.0	1.0(117)	2.2(4)	3.1(1)

Module	DRAM			FLASH			NVRAM		
	Total	Used	Free	Total	Used	Free	Total	Used	Free
2	32640K	11854K	20786K	8192K	3224K	4968K	512K	106K	406K

Uptime is 5 days, 20 hours, 14 minutes

show module 该命令给出Catalyst交换机各个插槽中的模块信息。

```
Console> (enable) show module
Mod Module-Name Ports Module-Type Model Serial-Num Status
-----
2 2 10/100BaseTX Supervis WS-X5530 008167898 ok
3 24 10/100BaseTX Ethernet WS-X5224 008161402 ok
5 12 10/100BaseTX Ethernet WS-X5203 008451509 ok
7 24 10/100BaseTX Ethernet WS-X5224 008161009 ok
10 24 10/100BaseTX Ethernet WS-X5224 008161288 ok
12 16 Token Ring WS-X5030 007380744 ok
```

Mod	MAC-Address(es)	Hw	Fw	Sw
-----	-----	----	----	-----

```

2 00-90-f2-a7-c1-00 thru 00-90-f2-a7-c4-ff 1.8 3.1(2) 3.1(1)
3 00-10-7b-2e-ca-e8 thru 00-10-7b-2e-ca-ff 1.3 3.1(1) 3.1(1)
5 00-10-7b-09-9a-50 thru 00-10-7b-09-9a-5b 1.1 3.1(1) 3.1(1)
7 00-10-7b-3d-be-f0 thru 00-10-7b-3d-bf-07 1.3 3.1(1) 3.1(1)
10 00-10-7b-3d-be-c0 thru 00-10-7b-3d-be-d7 1.3 3.1(1) 3.1(1)
12 00:05:77:05:86:42 thru 00:05:77:05:86:52 1.0 1.0(117) 3.1(1)

```

```

Mod      Sub-Type      Sub-Model      Sub-Serial      Sub-Hw
----      -
2        EARL 1+        WS-F5520       0008157389      1.1
2        uplink        WS-U5531       0008577601      1.1

```

show mac 该命令显示通过交换机的流量的详细统计信息。以下为摘录的其中三个端口的流量统计信息，包括每个端口接收和发送的数据帧、组播、单播和广播数据包的统计，错误信息统计，以及收/发字节总数统计等。

```

Console> (enable) show mac
MAC      Rcv-Frms      Xmit-Frms      Rcv-Multi      Xmit-Multi      Rcv-Broad      Xmit-Broad
-----
5/10     30948         251858         14649          251758          108            0
5/11     44490         166061         4953           145105          96             5774
5/12     43857         166409         4438           145408          15             5823

```

```

MAC      Dely-Excd      MTU-Excd      In-Discard      Lrn-Discrd      In-Lost      Out-Lost
-----
5/10     0              0             38              0               0            0
5/11     0              0             61              0               0            0
5/12     2              0             73              0               0            0

```

```

Port      Rcv-Unicast      Rcv-Multicast      Rcv-Broadcast
-----
5/10     16192            14649              108
5/11     39441            4953               96
5/12     39405            4438               15

```

```

Port      Xmit-Unicast      Xmit-Multicast      Xmit-Broadcast
-----
5/10      100              251764              0
5/11     15182            145107              5774
5/12     15178            145410              5823

```

```

Port      Rcv-Octet      Xmit-Octet
-----
5/10     3183207        23975586
5/11     20334264        27851660
5/12     20290059        27865755

```

```

Last-Time-Cleared
-----
Sun May 16 1999, 02:25:04

```

clear config all 该命令清除Catalyst交换机的所有配置，重新设置到厂家默认配置状态，在该状态中，所有端口都位于VLAN 1，Catalyst交换机的作用就是一个大的交换式集线器。

```

Console> (enable) clear config all
This command will clear all configuration in NVRAM.
This command will cause ifIndex to be reassigned on the next system startup.
Do you want to continue (y/n) [n]? y
.....
.....
.....

```

.....
.....
.....

System configuration cleared.

show port 该命令给出关于交换机的端口级配置的统计信息。Catalyst交换机能够自动检测各端口的速率和单双工工作方式，在下面的显示中，可以看出交换机自动对端口 5/11和5/12进行了配置，它们的状态相同，都已经连接了设备，都位于 VLAN 1，端口速率均为10Mbps，为半双工工作方式。

```
Console> (enable) sh port
```

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
5/1		notconnect	1	normal	auto	auto	10/100BaseTX
5/2		notconnect	1	normal	auto	auto	10/100BaseTX
5/3		notconnect	1	normal	auto	auto	10/100BaseTX
5/4		notconnect	1	normal	auto	auto	10/100BaseTX
5/5		notconnect	1	normal	auto	auto	10/100BaseTX
5/6		notconnect	1	normal	auto	auto	10/100BaseTX
5/7		notconnect	1	normal	auto	auto	10/100BaseTX
5/8		notconnect	1	normal	auto	auto	10/100BaseTX
5/9		notconnect	1	normal	auto	auto	10/100BaseTX
5/10		notconnect	1	normal	auto	auto	10/100BaseTX
5/11		connected	1	normal	a-half	a-10	10/100BaseTX
5/12		connected	1	normal	a-half	a-10	10/100BaseTX

show port slot/port 该命令就是在show port命令中加上了具体的端口号，它可以提供关于该端口的更丰富的信息。在下例中将看到了更多的信息，譬如该端口的 MAC级安全信息、以太网冲突信息和错误统计信息等。

```
Console> (enable) sh port 5/11
```

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
5/11		connected	1	normal	a-half	a-10	10/100BaseTX

Port	Security	Secure-Src-Addr	Last-Src-Addr	Shutdown	Trap
5/11	disabled			No	disabled

Port	Broadcast-Limit	Broadcast-Drop
5/11	-	0

Port	Status	Channel mode	Channel status	Neighbor device	Neighbor port
5/11	connected	auto	not channel		

Port	Align-Err	FCS-Err	Xmit-Err	Rcv-Err	UnderSize
5/11	0	0	0	0	0

Port	Single-Col	Multi-Coll	Late-Coll	Excess-Col	Carri-Sen	Runts	Giants
5/11	0	0	0	0	0	0	0

Last-Time-Cleared

Sun May 16 1999, 02:25:04

show cam dynamic 该命令是一个用户模式命令，它显示交换机所学到的与它相连的主机的MAC地址。

```
Console> (enable) show cam dynamic
```

VLAN	Dest MAC/Route Des	Destination Ports or VCs
2	00-e0-1e-9c-8e-b0	5/10
1	00-e0-1e-9c-8e-b0	5/10
2	00-10-7b-06-c2-c1	5/11
1	00-e0-1e-5b-27-61	5/12
1	00-00-ff-ff-ff-fb	1/4

Total Matching CAM Entries Displayed = 5

show system 该命令用于显示Catalyst交换机的系统信息，包括联系人、当前流量和峰值流量、系统运行时间和散热信息。

```
Console> (enable) show system
```

PS1-Status	PS2-Status	Fan-Status	Temp-Alarm	Sys-Status	Uptime d,h:m:s	Logout
ok	none	ok	off	ok	5,20:14:10	20 min

PS1-Type	PS2-Type	Modem	Baud	Traffic	Peak	Peak-Time
WS-C5508	none	disable	9600	0%	0%	Sun May 16 1999, 02:25:04

System Name	System Location	System Contact

set interface 该命令可设置用于带内访问的接口（SC0）的IP地址。

```
Console> (enable) set interface sc0 192.1.1.3
```

Interface sc0 IP address set.

show interface 该命令可显示Catalyst交换机内部用于带内访问和SLIP访问的接口的IP地址。

```
Console> (enable) sh interface
```

```
sl0: flags=51<UP,POINTOPOINT,RUNNING>
```

```
slip 0.0.0.0 dest 128.73.35.160
```

```
sc0: flags=63<UP,BROADCAST,RUNNING>
```

```
VLAN 1 inet 192.1.1.3 netmask 255.255.255.0 broadcast 192.1.1.255
```

set ip permit 该命令用于建立IP访问列表，Catalyst交换机根据它来访问对交换机的带内远程登录和SNMP访问，在IP访问列表中最多可定义10个IP地址。

```
Console> (enable) set ip permit 192.1.1.1
```

192.1.1.1 added to IP permit list.

show ip permit 该命令用于查看Catalyst交换机上配置的IP访问列表信息，以及是否有非法IP地址试图对交换机进行远程登录或SNMP访问。IP访问列表必须通过set ip permit enable命令来激活，可以使用命令set ip permit disable来取消IP访问列表。

```
Console> (enable) show ip permit
```

IP permit list feature enabled.

Permit List	Mask
192.1.1.1	

Denied IP Address	Last Accessed Time	Type
192.1.1.2	05/25/99, 14:25:50	Telnet

set port security 该命令用于配置Catalyst交换机的某端口，使它拒绝来自未预定义的MAC地址的数据流。下面的配置命令使端口5/12只接收来自MAC地址为00-e0-1e-5b-27-62的主机的数据流。端口安全属性可以用命令set port security 5/12 disable取消。

```
Console> (enable) set port security 5/12 enable 00-e0-1e-5b-27-62
```

Port 5/12 port security enabled with 00-e0-1e-5b-27-62 as the secure mac address

Trunking disabled for Port 5/12 due to Security Mode

show vtp domain 该命令用于显示交换机的 VTP域信息，为使 Catalyst交换机使用除 VLAN 1 外的其他 VLAN号，必须先给交换机设定一个域名。设定域名使用命令 set vtp domain。

```
Console> (enable) sh vtp domain
Domain Name          Domain Index    VTP Version    Local Mode    Password
-----
1                    2              server         -

Vlan-count    Max-vlan-storage    Config Revision    Notifications
-----
5              1023                0                  disabled

Last Updated    V2 Mode    Pruning    PruneEligible on Vlans
-----
0.0.0.0         disabled    disabled    2-1000
```

set vlan vlan_number slot_port , set vlan命令用于将某一端口划分到特定的 VLAN。下例为将端口 5/12 分配到 VLAN 2，VLAN 必须通过 set vlan 命令激活。

```
Console> (enable) set VLAN 2 5/12
VLAN 2 modified.
VLAN 1 modified.
VLAN    Mod/Ports
----
2      5/11-12
```

show vlan 该命令显示交换机上设置的所有 VLAN 的信息。

```
Console> (enable) sh vlan
VLAN    Name          Status    Mod/Ports, Vlans
----
1      default      active    2/1-2
          3/1-24
          5/1-10
          7/1-24
          10/1-24
2      VLAN0002     active    5/11-12
1002   fddi-default active
1003   token-ring-default active
1004   fddinet-default active
1005   trnet-default active

VLAN    Type    SAID    MTU    Parent    RingNo    BrdgNo    Stp    BrdgMode    Trans1    Trans2
----
1      enet    100001  1500  -          -          -          -          -          0          0
2      enet    100002  1500  -          -          -          -          -          0          0
1002   fddi    101002  1500  -          0x0        -          -          -          0          0
1003   trcrf   101003  1500  0          0x0        -          -          -          0          0
1004   fdnet   101004  1500  -          -          0x0        ieee    -          0          0
1005   trbrf   101005  1500  -          -          0x0        ibm     -          0          0

VLAN    AREHops    STEHops    Backup CRF
----
1003     7          7          off
```

show vlan vlan_number , 在 show vlan 命令后加上具体的 VLAN 号之后，将显示有关该 VLAN 的信息，包括 VLAN 的名称、状态、成员端口及一些统计信息。

```
Console> (enable) sh VLAN 2
VLAN    Name          Status    Mod/Ports, Vlans
----
2      VLAN0002     active    5/11-12
```

VLAN	Type	SAID	MTU	Parent	RingNo	BrdgNo	Stp	BrdgMode	Trans1	Trans2
2	enet	100002	1500	-	-	-	-	-	0	0

VLAN	AREHops	STEHops	Backup CRF
------	---------	---------	------------

set trunk 该命令将Catalyst交换机的端口设置为中继端口。

```
Console> (enable) set trunk 5/10 on
Port(s) 5/10 trunk mode set to on.
```

show trunk 该命令提供与交换机的中继有关的信息，包括该中继上哪些 VLAN是可以进入的，哪些VLAN当前处于激活状态。下面的显示说明，中继端口 5/10允许来自所有VLAN的数据流进入。

```
Console> (enable) sh trunk
Port      Mode      Status
-----
5/10      on        trunking
```

```
Port      Vlans allowed on trunk
-----
```

```
5/10      1-1005
```

```
Port      Vlans allowed and active in management domain
-----
```

```
5/10      1-2,1003,1005
```

```
Port      Vlans in spanning tree forwarding state and not pruned
-----
```

```
5/10      1-2,1003,1005
```

20.7 结论

本章着重讨论了Cisco局域网交换机家族中的一种——Catalyst 5500交换机的配置和运行，可以看到Catalyst交换机是一种支持虚拟局域网的交换式集线器，它还可以通过安装路由交换模块（RSM）从而集第二层的交换和第三层的路由于一体。

本章的实验中演示了Catalyst交换机的一些特性，包括MAC端口安全特性、IP访问列表、VLAN之间的路由和ISL中继等。