5 Catalyst 交换机三层接口配置与管理

上一章介绍了 Catalyst 交换机的二层接口属性配置，本章接着介绍 Catalyst 交换机的三层接口属性配置。相对二层接口而言，三层接口的属性配置与管理更为复杂，如本章要介绍的物理三层接口/逻辑三层接口、三层接口 IP 地址和默认网关、IP MTU、Fallback 桥接等配置与管理，交换机的 SNMP 管理，ARP、RARP 和 Proxy ARP 地址解析配置，以及 RIP、OSPF 两种在交换机中主要应用的动态路由基本配置。

另外，本章专门介绍了以太网通道（包括二层和三层以太网通道）的配置与管理。同样，还会涉及一些在后面各章中所介绍的技术和配置，如 VLAN、ACL 等，本章不进行具体介绍，参见后面各章的相关内容即可。

本章重点

- 三层接口的基本属性配置与管理
- SVI 接口及 IP MTU 和计数器配置
- 二层/三层以太网通道配置与管理
- SNMP 配置与管理
- RIP、OSPF 路由协议启动以及参数配置

5.1 配置 Cisco Catalyst 交换机三层接口

三层接口最大的特性就是可以配置像 IP 地址这样的三层属性，这样一来接口就可以通过 IP 地址由用户自己直接访问。三层接口的主要用途就是提供通信路由和可管理主机或者设备连接。

在上一章学习了 Cisco Catalyst 以太局域网交换机的各种接口类型，其中就说到本章将要具体介绍的 3 种三层接口类型：路由接口、SVI 接口和三层以太网通道接口。有关路由接口和 SVI 接口方面的基础知识分别参见 4.1.3 节和 4.1.4 节，而三层以太网通道接口方面的基础知识将在本章后面具体介绍。

5.1.1 理解三层接口

三层接口又分为物理三层接口和逻辑三层接口两大类：逻辑三层接口就是三层 VLAN 接口，它集成了路由和桥接双重功能；物理三层接口就只有路由功能，相当于传统的路由器。

1. 逻辑三层 VLAN 接口

逻辑三层 VLAN 接口为二层交换机的 VLAN 提供路由接口。传统意义上，网络需要一个从路由器到交换机连接的物理接口来完成 VLAN 路由，像 Catalyst 4500 系列这样的交换机通过集成的路由和桥接功能支持在单个 Catalyst 4500 系列交换机内部的 VLAN 间（inter-VLAN）路由。

图 5-1 所示为在传统网络中 3 个物理设备的路由和桥接功能是如何在一个 Catalyst 4500 系列交换机中完成的。在左边这个图中显示的是传统网络中实现 VLAN 间路由的拓扑结构，在这个结构中，是通过一个路由器（Router，连接二层交换机的两个 VLAN），右图显示的是通过 Catalyst 4500 系列交换机的逻辑三层 VLAN 接口来实现内部两个 VLAN 间的路由（其中的 Routing 功能是由 Catalyst 4500 系列交换机自身实现的），因为这个逻辑三层 VLAN 接口同时集成了路由和桥接功能。显然右边这种方案更具成本优势。

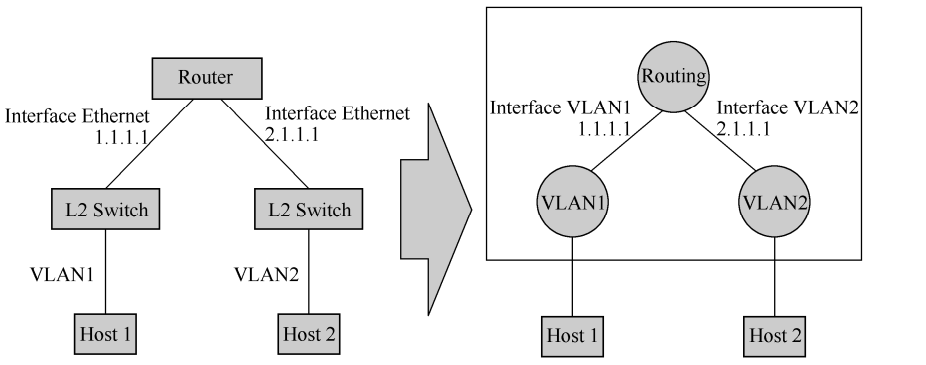

图 5-1 Catalyst 4500 系列交换机的逻辑三层 VLAN 接口实现 VLAN 路由的示例

【说明】有些模块结构的三层交换机就专门配置有 RSM（路由交换模块）或者 RSFC（路由交换功能卡），其目的就是为了在同一交换机内部不同 VLAN 之间实现二层交换和三层路由。这一点将在第 10 章介绍 VLAN 间路由时具体体现。

在逻辑三层接口中，还有一种接口类型，即前面提到的三层以太网通道接口，具体将在本章后面详细介绍。

2．物理三层接口

物理三层接口支持与传统路由器相当的功能。这些三层接口可以使 Catalyst 系列交换机直接连接可路由主机。图 5-2 所示为 Catalyst 4500 系列交换机是如何担当传统路由器角色的。图中的 Rourer 就是由 Catalyst 4500 系列交换机担当的，连接两台主机的接口就是物理三层路由接口。

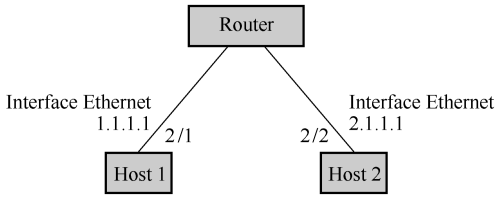

图 5-2　Catalyst 4500 系列交换机的物理三层接口的路由应用示例

5.1.2　三层接口的基本配置

三层交换机可以为每个路由端口和 SVI 接口分配 IP 地址。在一个交换机堆叠中可以配置的 SVI 接口和路由端口数是没有限制的。但是，SVI 接口数、路由端口数和所配置的其他特征数之间的相互关系会影响 CPU 的使用。如果交换机正在使用最大限度的硬件资源，试图创建路由端口和 SVI 端口，将可能出现以下结果：

- 如果试图创建一个新的路由端口，交换机会产生一条消息，提示没有足够的资源来转换接口为路由端口，接口将保持交换端口类型。
- 如果试图创建一个扩展范围的 VLAN，会产生一条错误消息，扩展 VLAN 的创建将被拒绝。
- 如果交换机接收到一个新的 VLAN 的 VTP 通告，则交换机将发送一条消息，提示没有足够的硬件资源可用，并且关闭该 VLAN。此时如果使用 **show vlan** 用户执行模式命令，则该命令的输出会显示这个 VLAN 处于待定状态。
- 如果交换机试图以配置有超过其硬件资源可以支持的 VLAN 和路由端口数重新启动，则 LVBAN 会创建，但是路由端口将关闭，而且交换机会发送一条消息，显示这是因为硬件资源不足造成的。

所有三层接口都需要一个 IP 地址来路由通信。但在配置 IP 属性之前，必须先在接口上启用 IP 路由，并且指定所用的 IP 路由协议。以下显示了如何配置一个接口为三层接口，并且显示如何为接口分配 IP 地址。

【注意】如果物理端口是二层模式（这是默认的），则必须键入 **no switchport** 接口配置命令来把该接口转换成三层模式。键入 **no switchport** 命令后，该接口先是关闭，然后重新开启，并且会在连接到该接口的设备上显示一条消息。另外，在把一个二层接口转换成三层接口后，该接口的当前配置信息都将丢失，恢复到默认设置。

表 5-1 所示为设置三层接口的步骤（自特权模式开始）。

表 5-1　设置三层接口的步骤

步骤	命令	用途说明
1	Switch# **configure terminal**	进入全局配置模式
2	Switch(config)# **interface** {{**fastethernet** | **gigabitethernet**} *interface-id*} | {**vlan** *vlan-id*} | {**port-channel** *port-channel-number*}	指定要配置成三层接口的接口，并进入接口配置模式。如果是路由接口，则指定具体的接口类型，如果是 SVI 接口，则指定具体的 VLAN ID
3	Switch(config-if)#**no switchport**	进入三层模式，仅适用于物理三层接口

续表

步骤	命令	用途说明
4	Switch(config-if)#**ip address** *ip_address subnet_mask*	为该接口配置 IP 地址和子网掩码
5	Switch(config-if)#**no shutdown**	打开接口
6	Switch(config-if)#**exit**	（可选）返回全局配置模式
7	Switch(config)#**ip default-gateway** *ip-address*	（可选）键入直接与交换机连接的下一跳路由器接口的 IP 地址，作为默认网关配置。默认网关从交换机上接收带有不可解析目的 IP 地址的 IP 数据包。 一旦配置了默认网关，交换机就可以与想要通信的远程网络主机建立连接。 在交换机配置了 IP 路由时，不再需要配置默认网关
8	Switch(config)#**end**	返回到特权模式
9	Switch# **show interfaces** [*interface-id*] Switch# **show ip interface** [*interface-id*] Switch# **show running-config interface** [*interface-id*]	校验以上设置
10	Switch# **copy running-config startup-config**	（可选）在配置文件中保存设置更改

要删除一个接口的 IP 地址，可以使用 **no ip address** 接口配置命令。

以下是一个显示如何配置一个端口为路由端口，并为该端口分配 IP 地址的示例。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.20.135.21 255.255.255.0
Switch(config-if)# no shutdown
```

以下示例显示了如何配置逻辑三层 VLAN 2 接口，并分配 IP 地址。

```
Switch> enable
Switch# config term
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)# vlan 2
Switch(config)# interface vlan 2
Switch(config-if)# ip address 10.1.1.1 255.255.255.248
Switch(config-if)# no shutdown
Switch(config-if)# end
```

以下示例显示了如何使用 **show interfaces** 命令显示上例配置的 IP 地址配置和三层 VLAN 2 接口状态。

```
Switch# show interfaces vlan 2
Vlan2 is up, line protocol is down
  Hardware is Ethernet SVI, address is 00D.588F.B604 (bia 00D.588F.B604)
  Internet address is 172.20.52.106/29
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
Switch#
```

以下示例显示了如何使用 **show running-config** 命令显示 VLAN 2 三层接口的 IP 地址配置。

```
Switch# show running-config
Building configuration...

Current configuration : !
interface Vlan2
 ip address 10.1.1.1 255.255.255.248
!
ip classless
no ip http server
!
!
line con 0
line aux 0
line vty 0 4
!
end
```

5.1.3　配置 SVI 自动状态排除

SVI 自动状态排除功能在以下端口配置发生改变时会关闭交换机的三层接口：

- 当一个 VLAN 中的最后一个端口关闭时，则这个 VLAN 三层接口将关闭。
- 当 VLAN 中的第一个端口启用时，则这个 VLAN 三层接口又将重新启用。

可以在一个访问或者中继模式端口上配置 SVI 自动状态排除（Autostate Exclude），以便在 SVI 接口状态（打开或者关闭）计算时排除该端口，即使这个端口与 SVI 属于同一个 VLAN。当被排除的端口处于打开状态，而 VLAN 中的所有其他端口是关闭状态时，SVI 接口状态也将为关闭状态。

在 VLAN 中至少有一个端口是处于打开状态，并且没有被排除，才能确定 SVI 线路状态为打开的。在确定 SVI 接口状态时，可以使用以下命令来排除监控端口状态。在 SVI 接口状态改变计算中排除端口的配置步骤如表 5-2 所示。

表 5-2　在 SVI 接口状态改变计算中排除端口的配置步骤

步骤	命令	用途说明
1	Switch# **configure terminal**	进入全局配置模式
2	Switch(config)# **interface** *interface-id*	指定要配置的二层接口（物理端口或者端口通道），并进入接口配置模式
3	Switch(config-if)#**switchport autostate exclude**	在定义 SVI 线路状态时排除以上访问或者中继端口，亦即在以上端口上启用 SVI 自动状态排除特征
4	Switch(config-if)#**end**	返回到特权模式
5	Switch#**show running config interface** *interface-id* Switch#**show interface** *interface-id* **switchport**	（可选）显示指定接口的运行配置 （可选）显示指定接口的交换端口配置
6	Switch#**copy running-config startup-config**	（可选）在配置文件中保存以上设置更改

以下示例显示了如何在 g3/1 接口上应用 SVI 自动状态排除功能。

```
Switch# conf terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)# interface g3/1
Switch(config-if)# switchport autostate exclude
Switch(config-if)# end
```

以下示例显示了如何查看 g3/4 接口运行配置。

```
Switch# show run int g3/4
Building configuration...

Current configuration : 162 bytes
!
```

```
interface GigabitEthernet3/4
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,3
 switchport autostate exclude                                    <=====
 switchport mode trunk
end
```

以下示例显示了 g3/4 接口的交换端口配置。

```
Switch# show int g3/4 switchport
Name: Gi3/4
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On Access Mode VLAN: 1 (default) Trunking Native Mode VLAN: 1
(default) Administrative Native VLAN tagging: enabled Voice VLAN: none Administrative
private-vlan host-association: none Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none Administrative private-vlan trunk
Native VLAN tagging: enabled Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none Administrative private-vlan trunk
associations: none Administrative private-vlan trunk mappings: none Operational
private-vlan: none Trunking VLANs Enabled: 2,3 Pruning VLANs Enabled: 2-1001 Capture Mode
Disabled Capture VLANs Allowed: ALL
Autostate mode exclude                                          <=====

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch#
```


5.1.4 配置三层接口 IP MTU

MTU（Maximum Transmission Unit，最大传输单元）就是指端口上可以接收的最大数据包大小，超过这个大小的数据包，端口就会拒绝接收或者丢弃。在以太网交换机和交换机堆叠中接收和传输帧的默认 MTU 大小为 1500 B。可以通过使用 **system mtu** 全局配置命令为所有工作于 10Mb/s 或者 100Mb/s 的接口提高 MTU；通过使用 **system mtu jumbo**（ **jumbo** 关键字是指大的意思）全局配置命令为所有工作于 1000Mb/s 的接口提高 MTU；也可以通过 **system mtu routing** 全局配置命令仅为路由端口改变 MTU 大小设置。

【注意】不能配置一个路由 MTU 大小超过系统 MTU （system mtu）大小。如果改变系统 MTU 大小比当前配置的路由 MTU 大小更小的值，配置是接受了，但是不会应用，直到下次交换机重置。当配置改变生效后，路由 MTU 大小自动默认为新的系统 MTU 大小值。千兆以太网端口不受 **system mtu** 命令配置影响，而 10/100Mb/s 端口不受 **system mtu jumbo** 命令配置影响。但是，如果没有使用 **system mtu jumbo** 命令对千兆端口 MTU 大小进行设置，则 **system mtu** 命令的设置将应用到所有千兆以太网接口。

不能为个别接口设置 MTU 大小，只能为交换机或交换机堆叠中的所有 10/100 Mb/s 或者千兆以太网接口统一设置。当改变系统 MTU 或者 jumbo MTU（大尺寸 MTU）大小时，在新配置生效前必须重置交换机。但是 **system mtu routing** 命令的配置不需要重置交换机即可生效。

交换机 CPU 接收帧的大小限制为最高 1998B，而不管使用 **system mtu** 或者 **system mtu jumbo** 命令所进行的设置如何。尽管超出这个限制的帧仍可以转发和路由，但不能由 CPU 接收。由 CPU 接收的帧包括流量控制、SMNP、Telnet 或者路由协议等帧类型。

路由包会按照路由接口的 MTU 设置进行检查。路由端口的 MTU 值设置是从应用的 **system mtu** 设置的值（而不是从 **system mtu jumbo** 命令设置的值）传递的。也就是说，路由 MTU 永远不

可能大于系统 MTU 设置。在与邻居接口协商链路 MTU 时，路由协议使用系统 MTU 值。例如，OSPF（Open Shortest Path First，开放最短路径优先）协议在与邻居路由器建立连接前使用这个 MTU 值。要查看指定 VLAN 的路由包的 MTU 值设置，可以使用 **show platform port-asic mvid** 特权模式命令。

【注意】如果二层千兆以太网接口被配置了接受大于 10/100 Mb/s 接口限制的帧，则在千兆二层以太网接口上接收的和在二层 10/100 Mb/s 接口上发送的大尺寸帧都将被丢弃。

为所有 10/100 Mb/s 和千兆以太网接口配置 MTU 大小的步骤如表 5-3 所示。

表 5-3　为所有 10/100 Mb/s 和千兆以太网接口配置 MTU 大小的步骤

步骤	命令	用途说明
1	Switch#**configure terminal**	进入全局配置模式
2	Switch(config)#**system mtu** *bytes*	（可选）为所有工作于 10 或者 100Mb/s 的二层以太网接口设置 MTU 值，范围是 1500B～1998B，默认是 1500B
3	Switch(config)#**system mtu jumbo** *bytes*	（可选）为所有工作于 1000Mb/s 的二层以太网接口设置 MTU 值，范围是 1500B～9000B，默认是 1500B
4	Switch(config)#**system mtu routing** *bytes*	（可选）为路由端口设置 MTU 值，范围是 1500B～第 2 步设置的系统 MTU 值。默认是 1500B。尽管大于这个 MTU 值的数据包可以被接收，但是不能被路由
5	Switch(config)#**end**	返回到特权模式
6	Switch#**copy running-config startup-config**	在启动配置文件中保存以上设置
7	Switch#**reload**	重载交换机系统

如果键入的值不在相应类型接口允许的范围内，则这个值设置将不被接受。一旦交换机重载，则可以通过键入 **show system mtu** 特权模式命令校验你的设置。

以下示例显示了如何为千兆以太网接口设置 MTU 值为 1800 B。

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

以下示例显示了试图设置千兆以太网接口一个不在该类接口允许范围内的 MTU 值（25000 Mb/s）时的响应——% Invalid input detected at '^' marker（在标记位置的输入无效）。

```
Switch(config)# system mtu jumbo 25000
                                 ^
% Invalid input detected at '^' marker.
```

以下示例显示了如何为 VLAN 1 接口配置 IPv4 MTU 值为 68，然后再校验以上设置是否生效。

```
Switch# configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if)# ip mtu 68
Switch(config-if)# end
Switch# show ip interface vlan 1
Vlan1 is up, line protocol is up
  Internet address is 10.10.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 68 bytes
  Helper address is not set
  …
```

5.1.5　配置三层接口计数器

接口计数器用来记录接口各种属性的统计信息，如各接口流入/流出通信量、接口 ID 编号、VLAN ID 编号、日志信息等。默认是未配置的，也就是没有启用的。

当从交换机上移去一个线路卡时，线路卡上端口当前启用的三层计数器将呈未配置状态。这就

意味着，在重新插入这块线路卡时必须重新配置线路卡中的三层端口。注意，**Supervisor Engine 6-E 模块不支持接口计数器配置**。配置三层接口计数器的步骤如表 5-4 所示。

表 5-4　配置三层接口计数器的步骤

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*	指定要配置的三层接口，并进入接口配置模式
3	Switch(config-if)# **counter**	启用三层接口计数器
4	Switch(config)# **end**	退出全局配置模式
5	Switch# **show run interface** *interface-id*	显示当前运行文件中的以上设置

以下示例显示了如何启用并显示 VLAN 1 接口上的计数器。

```
Switch# configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if)# counter
Switch(config-if)# end
Switch#
00:17:15: %SYS-5-CONFIG_I: Configured from console by console
Switch# show run interface vlan 1
Building configuration...

Current configuration : 63 bytes
!
interface Vlan1
 ip address 10.0.0.1 255.0.0.0
 counter
end
```

要删除计数器，可以使用 **no counter** 接口配置命令。如果计数器到达了设置的最大值，**counter** 命令失效，并且显示错误消息。下面是一个具体示例（错误消息提示在自倒数第 6 行开始）。

```
Switch# config terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)# interface fa3/2
Switch(config-if)# no switchport
Switch(config-if)# counter
 Counter resource exhausted
Switch(config-if)# end
Switch#
00:24:18: %SYS-5-CONFIG_I: Configured from console by console

In this situation, you must release a counter from another interface for use by the new interface.
```

5.2　以太网通道基础

本节将介绍如何在 Cisco Ctalyst 交换机的二层和三层端口上配置以太网通道（**也就是说有二层以太网通道和三层以太网通道之分**）。以太网通道可以为交换机、路由器和服务器间提供高速容错链路。可以用它来提高配线室和数据中心间的带宽，也可以在网络中任何认为有可能出现性能瓶颈的位置中部署它。

以太网通道通过重新分配负载，在当前可用的链路上恢复失效的链路。如果一个链路失效了，以太网通道会自动重定向失效途径链路上的通信到正常工作的链路上。

5.2.1　以太网通道概述

如图 5-3 所示是由多个千兆以太网链路捆绑在一起，形成的一个单一逻辑链路的以太网通道的典型示例。

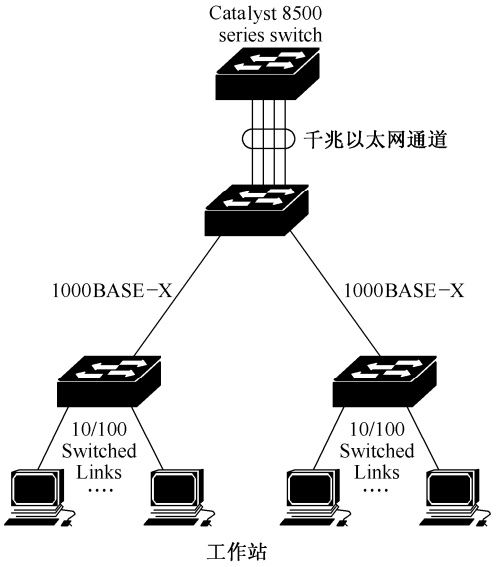

图 5-3　一个典型的千兆以太网通道示例

一个快速以太网通道最高可以在交换机和其他交换机或者主机间提供 800 Mb/s 的全双工带宽（实际上是 1.6Gb/s），而一个千兆以太网通道可以在交换机和其他交换机或者主机间提供最高 8Gb/s（实际上是 16Gb/s）的带宽。但要注意，以上所说的都是基于双绞线以太网端口的，因为光纤通道不支持全双工配置，所以最高支持的带宽也就在以上基础上减半了。

每个以太网通道可以包括最多 8 个适当配置的以太网端口，以太网通道中的所有端口都必须配置为二层或者三层端口。交换机可以创建的以太网通道的数量因为不同系列而有所不同，如在 Catalyst 3750 及以前系列的 Cisco 交换机中，以太网通道的数量限制为最多 48 个，而 Catalyst 4500 系列则允许最多配置 64 个以太网通道，在 Catalyst 6500 系列则允许最多有 128 个以太网通道，具体参见相应产品的说明书。三层以太网通道端口是由路由端口组成的。路由端口是物理接口通过 **no switchport** 接口配置命令配置成三层端口的。

可以手动配置以太网通道，也可以用以下两种协议来自动形成以太网通道：PAgP（Port Aggregation Protocol，端口汇聚协议）、LACP（Link Aggregation Control Protoco，链路汇聚控制协议）。但是以太网通道中的两端必须是相同协议的。PAgP 是 Cisco 专有的协议，而 LACP 是在 IEEE 802.3ad 标准中定义的。

PAgP 与 LACP 相互不兼容，也就是说在一个以太网通道中不能同时存在这两种协议。当在 PAgP 或者 LACP 模式下配置一端的以太网通道时，系统会自动与以太网通道的另一端协商，以决定激活哪个端口。通道中的其余端口被置于暂停状态。自 Cisco IOS 12.2(35)SE 版本开始，取代了挂起状态（Suspended State），本地端口被置于独立状态（Independent State），可以继续承载数据通信，就像其他单一链路端口一样。通道中的这些端口配置没有改变，但它们不再参与到以太网通道中。

表 5-5 所示为用户可配置的以太网通道模式。

当在 **on** 模式下配置以太网通道时，不会发生协商，交换机强迫所有端口在以太网通道中成为活动模式。

表 5-5　以太网通道模式

模式	描述
on	强制 LAN 端口加入到通道中。在这种 on 模式中，仅当一个 on 模式的 LAN 端口组与另一个配置为 on 模式的 LAN 端口组连接时才会存在一个可用的以太网通道。因为配置为 on 模式的端口不会与邻接接口协商，在两个端口之间没有协商通信。不能在以太网通道协议（PAgP 或者 LACP）上配置 on 模式。如果一端用户是配置为 on 模式，则另一端必须也是 on 模式
auto	PAgP 协议的一种模式。它把 LAN 端口置于被动协商状态。端口可以响应接收到的 PAgP 包，但不能发送 PAgP 包与其他端口进行协商。这种设置可以最大限度地减少 PAgP 包的传输。但这种模式在以太网通道中的端口成员来自交换机堆叠中的不同成员交换机时不支持。也就是在交叉堆叠以太网通道（也就是以太网通道中的端口来自堆叠中不同的交换机）中不支持 **auto** 模式
desirable	PAgP 协议的一种模式。它把端口置为主动协商状态，端口可以发送 PAgP 包主动与其他端口进行协商。这种模式在以太网通道中的端口成员来自交换机堆叠中的不同成员交换机时也不支持，亦即在交叉堆叠以太网通道中不支持 **desirable** 模式
passive	LACP 协议的一种模式。它把端口置于被动协商状态。这种模式的端口响应接收到的 LACP 包，但不发起 LACP 协商。这是默认的模式
active	LACP 协议的一种模式。它把端口置于主动协商状态。这种模式的端口通过发送 LACP 包，发起与邻接端口进行协商

可以在一个独立交换机上，或者在交换机堆叠中的单一交换机上，或者交换机堆叠中的多个交换机上创建以太网通道。如图 5-4 所示是通道端口都是在单一交换机上创建的以太网通道，而图 5-5 所示为通道端口跨越交换机堆叠中多台交换机的以太网通道。

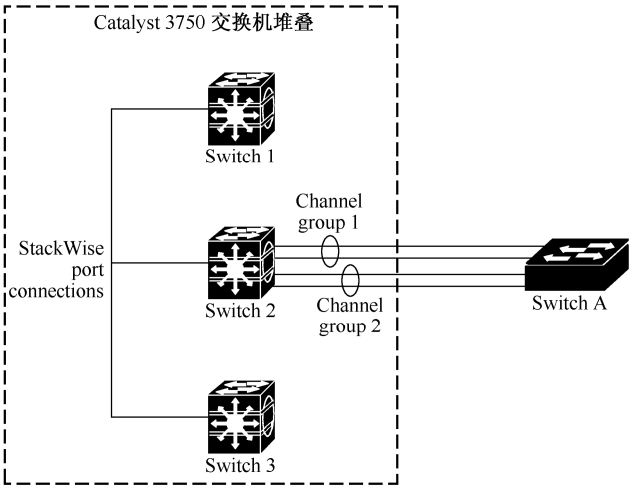

图 5-4　单一交换机上的以太网通道示例

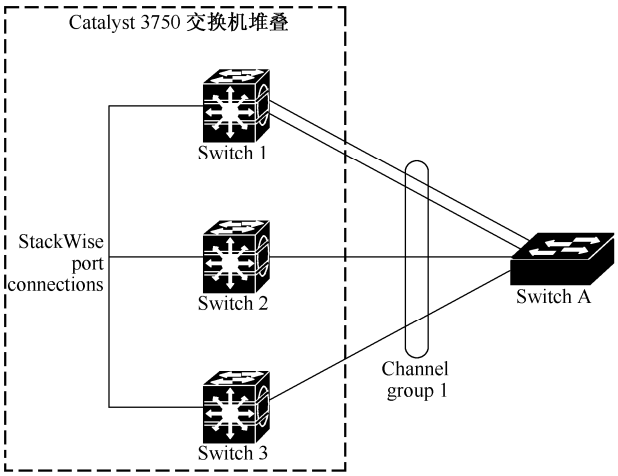

图 5-5　跨越堆叠的以太网通道示例

如果以太网通道中的一条链路失效，则原先这条链路上的流量会自动转移到以太网通道中其他正常工作的链路上。如果在交换机上启用了跟踪功能，则以太网通道会为链路失效发送一个 trap 信息，以标识这条链路失败的交换机、以太网通道和失效链路。在以太网通道中的一个链路上流入的广播和多播包是阻止再从以太网通道中的其他任何链路上返回的。

5.2.2　端口通道接口

当创建了以太网通道时，一个端口通道（Port-Channel）逻辑接口就自动生成了。对于二层端口，可以使用 **channel-group** 接口配置命令来动态创建端口通道逻辑接口。也可以使用 **interface port-channel** *port-channel-number* 全局配置命令手动创建端口通道逻辑接口，但是必须使用 **channel-group** *channel-group-number* 命令来把逻辑接口与一物理接口进行绑定。参数 *channel-group-number* 可以与参数 *port-channel-number* 一致，也可以使用新的号码。如果使用新的号码，则 **channel-group** 命令会动态创建一个新的端口通道，所以建议两者是相同的。

对于三层端口，应当通过 **nterface port-channel** 全局配置命令手动创建这个逻辑接口，然后再使用 **no switchport** 命令把逻辑端口也转换成三层端口。然后可以使用 **channel-group** 接口配置命令手动把这个接口指派到以太网通道中。

对于二层和三层端口，都可以使用 **channel-group** 命令绑定物理端口和逻辑端口，如图 5-6 所示。

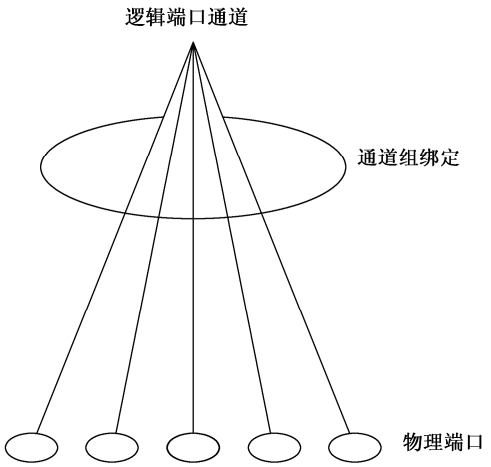

图 5-6　物理端口、逻辑端口通道和通道组之间的关系

每个以太网通道有一个端口通道逻辑接口，编号范围是 1～48（此处是针对 Catalyst 3750 及以前系列交换机而言的，对于像 Catalyst 6500 系列交换机可以允许最多创建 128 个以太网通道，编号范围为 1～128）。端口通道接口号是在 **channel-group** 接口配置命令中指定的。

在配置了以太网通道后，在端口通道中所发生的配置改变将应用到所有指派到端口通道接口的物理端口。物理端口仅在端口通道中的配置应用后才会应用。要改变在以太网通道中的所有端口的参数，只需应用配置命令到端口通道接口即可。

5.2.3　端口聚合协议（PAgP）

端口聚合协议（Port Aggregation Protocol，PAgP）是思科的专用协议，仅可以运行在 Cisco 交换机或者支持 PAgP 的第三方交换机上。PAgP 通过在以太网端口间交换 PAgP 包，可以使得以太网

通道自动创建更加容易。仅可以在单一交换机的以太网通道中使用 PAgP，而不能在跨越交换机堆叠的以太网通道中使用它。

通过使用 PAgP，交换机或者交换机堆叠会学习到每个伙伴端口对 PAgP 的支持以及性能。然后它动态地组合类似端口（如果是交换机堆叠，则仅限于同一台交换机上的端口）成为一个单一逻辑链路（也可以称为“逻辑通道”或者“逻辑聚合端口”）。相似配置端口的组合是基于硬件、管理属性和所包含的端口参数确定的。例如，PAgP 组合具有相同速率、双工模式、本地 VLAN、VLAN 范围，以及中继状态和类型的端口。然后组合这些端口的链路成为一个以太网通道，PAgP 以单一交换端口方式把端口组添加到生成树中。

交换端口仅与配置为 **auto** 或者 **desirable** 的相邻端口交换 PAgP 包，配置为 **on** 模式的端口不交换 PAaP 包。**Auto** 和 **desirable PAgP** 模式允许 PAgP 协议在 LAN 端口之间进行协商，例如端口速率，以决定它们是否可以形成一个以太网通道。对于二层以太网通道，也要考虑中继状态和所属 VLAN 号。有关以太网端口的模式参见表 5-7。

当 LAN 端口工作在不同的 PAgP 模式，且这些模式之间是兼容的时，则可以形成一个以太网通道。例如：

- 一个工作于 **desirable** 模式的 LAN 端口就可以与另一个同样工作于 **desirable** 模式的 LAN 端口成功形成一个以太网通道。
- 一个工作于 **desirable** 模式的 LAN 端口可以与另一个工作于 **auto** 模式的 LAN 端口形成一个以太网通道。
- 一个工作于 **auto** 模式的 LAN 端口不能与另一个工作于 **auto** 模式的 LAN 端口形成一个以太网通道，因为这两个工作于 **auto** 模式的端口都不能发起 PAgP 协商（因为 **auto PAgP** 模式只是能被动地与邻接接口协商）。

5.2.4 链路聚合控制协议（LACP）

LACP 是在 IEEE 802.3ad 标准中定义的，可以 Cisco 交换机管理跨越多台支持 IEEE 802.3ad 标准的交换机的以太网通道。LACP 通过在以太网端口间交换 LACP 包，使得自动创建以太网通道更加容易。

与 PAgP 一样，通过使用 LACP 协议，交换机或者交换机堆叠可以学习到支持 LACP 伙伴的标识和每个端口的性能，然后动态地组合相似配置的端口，形成一个单一逻辑链路（或者称“逻辑通道”、“逻辑聚合端口”）。相似配置的端口的识别基于硬件、管理属性、包含的端口参数。例如，LACP 组合具有相同速率、双工模式、本地 VLAN、VLAN 范围，以及中继状态和类型的端口。然后组合这些端口的链路成为一个以太网通道，LACP 以单一交换端口方式把端口组添加到生成树中。

active 和 **passive LACP** 模式（参见表 5-7）允许 PAgP 协议在 LAN 端口之间进行协商，例如端口速率，以决定它们是否可以形成一个以太网通道。对于二层以太网通道，也要考虑中继状态和所属 VLAN 号。

当 LAN 端口工作在不同的 LACP 模式，且这些模式之间是兼容的时，则可以形成一个以太网通道。例如：

- 一个工作于 **active** 模式的 LAN 端口就可以与另一个同样工作于 **active** 或者 **passive** 模式的 LAN 端口成功形成一个以太网通道。
- 一个工作于 **passive** 模式的 LAN 端口不能与另一个工作于 **passive** 模式的 LAN 端口形成一个以太网通道，因为这两个工作于 **passive** 模式的端口都不能发起 LACP 协商（因为 **passive LACP** 模式只是能被动地与邻接接口协商）。

5.2.5　负载均衡和转发方法

以太网通道可以均衡穿过通道中链路的负载流量。可以采用的均衡方案有多种：可以基于 MAC 地或者 IP 地址，也可以基于源或目的地址，或者基于源和目的地址两者。选择的方案将应用到交换机上的所有配置的以太网通道上。可以使用 **port-channel load-balance** 全局配置命令配置负载均衡和转发方法。

（1）基于源 MAC 地址。

以基于源 MAC 地址为标准转发到达以太网通道中的数据包。数据包是基于接收到的数据包中的源 MAC 地址分配在各以太网通道端口进行转发的。这样一来，来自不同主机的数据包将在以太网通道中的不同端口上进行转发，但是来自同一个 MAC 地址主机的数据包采用相同的端口进行转发，以此来实现负载均衡。

（2）基于目的 MAC 地址。

以基于目的 MAC 地址为标准转发到达以太网通道中的数据包。数据包是基于接收到的数据包中的目的主机 MAC 地址分配在各以太网通道端口进行转发的。这样一来，到达同一个 MAC 地址的数据包将在以太网通道中的同一个端口上进行转发，不同目的 MAC 地址的数据包采用不同端口进行转发，以此来实现负载均衡。

（3）基于源和目的 MAC 地址。

以基于源和目的 MAC 地址为标准转发到达以太网通道中的数据包。数据包是基于接收到的数据包中的源和目的 MAC 地址分配在各以太网通道端口进行转发的。这种转发方法是一种结合源和目的 MAC 地址进行负载分配的转发方法。这在不清楚在特定交换机上是采用基于源 MAC 地址转发还是采用基于目的 MAC 地址进行转发更适合时可以采用。在这种基于源和目的 MAC 地址的均衡方法中，从主机 A 到达主机 B、主机 A 到达主机 C，以及主机 C 到达主机 B 的数据包可以使用通道中不同的端口进行转发。

（4）基于源 IP 地址。

以基于源 IP 地址为标准转发到达以太网通道中的数据包。数据包是基于接收到的数据包中的源 IP 地址分配在各以太网通道端口进行转发的。这样一来，来自不同 IP 地址的数据包将在以太网通道中的不同端口上进行转发，以此来实现负载均衡。但是来自同一个源地址但目的地址不一样的数据包总是在通道的同一个端口上发送。

（5）基于目的 IP 地址。

以基于目的 IP 地址为标准转发到达以太网通道中的数据包。数据包是基于接收到的数据包中的目的 IP 地址分配在各以太网通道端口进行转发的。这样一来，来自同一个源地址而要发送到不同目的 IP 地址的数据包将在通道中的不同端口上发送，以此来实现负载均衡。但是来自不同源地址但目的地址一样的数据包总是在通道的同一个端口上发送。

（6）基于源和目的 IP 地址。

以基于源和目的 IP 地址为标准转发到达以太网通道中的数据包。数据包是基于接收到的数据包中的源和目的 IP 地址分配在各以太网通道端口进行转发的。这种转发方法是一种结合源和目的 IP 地址进行负载分配的转发方法。这在不清楚在特定交换机上是采用基于源 IP 地址转发还是采用基于目的 IP 地址进行转发更适合时可以采用。在这种基于源和目的 IP 地址的均衡方法中，从 IP 地址 A 到达 IP 地址 B、IP 地址 A 到达 IP 地址 C，以及 IP 地址 C 到达 IP 地址 B 的数据包可以使用通道中不同的端口进行转发。

不同的负载均衡方法各具优势，选择具体的均衡方法要依据交换机在网络中的位置，以及所要均衡的负载流量类型。在图 5-7 中，在以太网通道中，负载流量是 4 台工作站与一个路由器之间的

聚合通信。因为路由器是单一 MAC 地址设备，在交换机以太网通道中采用基于源 MAC 或 IP 地址的负载均衡方法，可以确保交换机充分利用到路由器的带宽，而在路由器的以太网通道中则可以采用基于目的 MAC 或 IP 地址的均衡方法，可以确保从路由器发出的流量可以均衡地分配到所连接的 4 台工作站上。

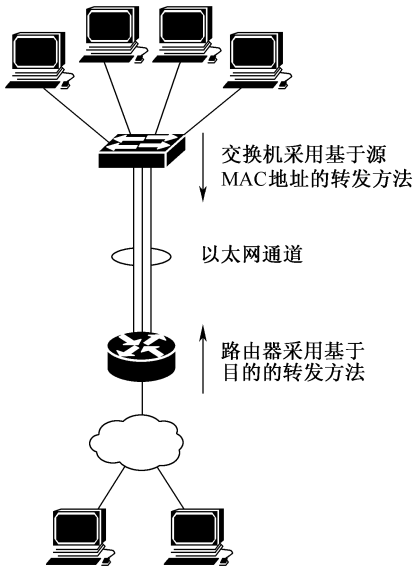

图 5-7　负载均衡和转发方法示例

通过以上几种可选的均衡方案，可以提供灵活的方案选择。例如，如果在一个通道中的流量是仅到一个单一 MAC（如路由器），如果选用基于目的 MAC 地址均衡方案，则流量总是会在同一个链路中传输，达不到均衡的目的。此时选用基于源或者目的 IP 地址的均衡方案可能会更好。

5.3　配置以太网通道

上节介绍了以太网通道的基础知识及以太网通道的主要应用，本节要介绍的是以太网通道创建和应用的具体配置方法，主要包括以下几方面的内容：

- 默认以太网通道配置。
- 以太网通道配置指南。
- 配置二层以太网通道（必需）。
- 配置三层以太网通道（必需）。
- 配置以太网通道负载均衡（可选）。
- 配置 PAgP 学习模式和优先权（可选）。
- 配置 LACP 热备份端口（可选）。

5.3.1　默认的以太网通道配置

在为新创建的以太网通道进行配置前，最好先了解一下以太网通道的默认配置，以便有针对性地进行配置修改。在创建了以太网通道后，默认的以太网通道配置如表 5-6 所示。

表 5-6　默认以太网通道配置

特征	默认设置
通道组	没有分配
端口通道逻辑接口	没有定义
PAgP 模式	无默认
PAgP 学习方法	在所有端口上聚合端口学习
PAgP 优先权	所有端口的 PAgP 优先权均为 128
LACP 模式	无默认
LACP 学习方法	在所有端口上聚合端口学习
LACP 端口优先权	所有端口 LCAP 优先权均为 32768
LACP 系统优先权	32768
LACP 系统 ID	LCAP 系统优先权和堆叠 MAC 地址
负载均衡	基于流入包中源 MAC 地址的交换机负载分配

5.3.2　以太网通道配置指南

如果配置不适当，一些以太网通道端口会自动禁用，以避免网络环路和其他问题发生。所以，建议在配置以太网通道时参考以下配置指南：

- 在 Catalyst 3750 等早期系列交换机堆叠中不要试图配置超过 48 个以太网通道，而在像 Catalyst 6500 等中高档系列交换机中，最多可以创建 128 个以太网通道。
- 最多配置包括 8 个同类型的以太网端口的 PAgP 以太网通道。
- 最多配置包括 16 个同类型的以太网端口的 LACP 以太网通道。其中最多 8 个端口可以被激活，8 个端口处于待机模式。
- 最多可配置包括两个 10G 以太网模块端口的交叉堆叠以太网通道。
- 为在一个以太网通道中的所有端口配置相同速率的双工模式。
- 启用以太网通道中的所有端口。通过使用 **shutdown** 接口配置命令禁用以太网通道中的端口，则相应的链路就会失效，它上面的负载将转移到以太网通道其他正常工作的端口链路上。
- 当第一个组创建后，随后加入到这个组的所有端口参数都将按第一个端口中的参数设置。如果改变以下这些参数中的一个，则必须对组中的所有端口同时改变：
  - 允许的 VLAN 列表
  - 每个 VLAN 的生成树路径开销
  - 每个 VLAN 的生成树端口优先权开销
  - 生成树端口快速设置
- 不要配置一个端口属于多个以太网通道组。
- 不要配置一个以太网通道同时工作于 PAgP 和 LACP 模式。但是运行 PAgP 和 LACP 模式的以太网通道组可以在同一台或交换机堆叠中的不同交换机中共存。对于具体的以太网通道组来说，可以运行 PAgP 或者 LACP 模式，但不能同时运行。
- 不要配置一个交换端口分析仪（如 sniffer、科来分析仪等）目标端口作为一个以太网通道的一部分。
- 不要配置一个安全端口作为一个以太网端口的一部分，或者相反。
- 不要配置一个私有 VLAN 端口作为一个以太网通道的一部分。
- 不要配置一个以太网通道中的一个活动或者非活动成员端口作为 IEEE 802.1x 端口。如果在以太网通道端口上启用 IEEE 802.1x 协议，将弹出错误消息，也将不能启用成功。

【说明】在 Cisco IOS 12.2(18)SE 版本以前，如果在以太网通道的活动端口上启用 IEEE 802.1x 协议，则这个端口不加入到以太网通道中。

- 如果在交换接口上配置以太网通道，则在交换机上通过 **dot1x system-auth-control** 全局配置命令全局启用 IEEE 802.1x 协议之前从接口中删除以太网配置。
- 对于二层以太网通道，还需要注意：
  - 分配所有在以太网通道中的端口到同一个 VLAN 中，或者把它们配置为中继端口。属于不同本地 VLAN 的端口不能位于同一个以太网通道中。
  - 如果从中继端口上配置以太网通道，则需要校验这些中继端口上的中继模式（ISL 或者 IEEE 802.1Q）是否相同。在以太网通道端口中的不一致中继模式可能会出现意想不到的结果。
  - 在一个中继二层以太网通道中的所有端口支持相同的 VLAN 范围许可。如果 VLAN 许可范围不一致，则端口不属于以太网通道，即使 PAgP 设置成 **auto** 或者 **desirable** 模式。
  - 如果以太网通道中的端口在其他方面具有适当的配置，则以太网通道中的端口可以具有不同的生成树路径开销。
- 对于三层以太网通道，分配三层地址到端口通道逻辑接口上，而不是分配到通道中的物理端口上。
- 对于交叉堆叠以太网通道配置，要确保以太网通道中的所有端口要么通过配置为 LACP 模式指向以太网通道，要么通过使用 **channel-group** *channel-group-number* **mode on** 接口配置命令手动配置它们到同一个通道组。在交叉堆叠以太网通道中，不支持 PAgP 协议模式。

5.3.3 配置二层以太网通道

可以通过使用 **channel-group** 接口配置命令分配端口到通道组来配置二层以太网通道。这个命令会自动创建端口通道逻辑接口。

如果在端口上启用 PAgP 协议为 **auto** 或者 **desirable** 模式，则必须在添加端口到交叉堆叠以太网通道前重新配置它要么运行于 **on** 模式，要么运行于 LACP 模式。在交叉堆叠以太网通道中，不支持 PAgP 协议模式。

按照表 5-7 所示的步骤分配二层以太网端口到二层以太网通道中（自特权模式开始）。

表 5-7 配置二层以太网通道的步骤

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*	指定要添加到以太网通道的一个物理端口，并进入接口配置模式。 对于 PAgP 模式以太网通道可以最多配置 8 个相同类型、相同速率的端口到同一个以太网通道中。 对于 LACP 模式以太网通道可以最多配置 16 个相同类型、相同速率的端口到同一个以太网通道中。其中最多 8 个处于活动状态，其他的为待机状态
3	Switch(config-if)#**switchport mode** {**access** | **trunk**}	分配所有端口作为同一个 VLAN 中的静态访问端口，或者配置它们为中继端口
	Switch(config-if)#**switchport access vlan** *vlan-id*	如果配置端口作为静态访问端口，分配它们到同一个 VLAN 中，VLAN ID 范围是 1～4094
4	Catalyst 3750 及以前系列：Switch(config-if)#**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on**} | {**active** | **passive**} Catalyst 4000 及以后系列：Switch(config-if)#**channel-group** *port_channel_number* **mode** {**active** | **on** | **auto** | **passive** | **desirable**}	分配端口到通道组，并且指定是工作于 PAgP 模式还是 LACP 模式 参数 *channel-group-number* 用来指定通道组号，范围是 1～48（此处是针对 Catalyst 3750 及早期其他系列交换机而言的，如果是像 Catlyst 6500 等中高档交换机系列，则可以最多创建 128 个以太网通道，具体参见相应产品说明书）。 **mode** 关键字中的可选项说明如下： • **auto**：仅当检测到一个 PAgP 设备时启用 PAgP。它将把端口置于被动协商状态，对所接收到的 PAgP 包进行响应，但不会发送 PAgP 包进行协商。该可选项在以太网通道成员来自交换机堆叠中的不同交换机时不支持。

续表

步骤	命令	用途说明
4	Catalyst 3750 及以前系列：Switch(config-if)#**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on**} | {**active** | **passive**} Catalyst 4000 及以后系列：Switch(config-if)#**channel-group** *port_channel_number* **mode** {**active** | **on** | **auto** | **passive** | **desirable**}	• **desirable**：无条件地启用 PAgP 模式。它将把端口置于主动协商状态。该端口会主动发送 PAgP 包与其他端口进行协商。该可选项在以太网通道成员来自交换机堆叠中的不同交换机时也不支持。 • **on**：强迫通道中的端口不启用 PAgP 或者 LACP 协议。在 **on** 模式下，仅当一个 **on** 模式端口组与另一个 **on** 模式端口组连接时，才可能形成以太网通道。 • **non-silent**：（可选）如果你的交换机是与一个支持 PAgP 协议的交换机连接，则配置这个交换机端口为 **non-silent**（非沉寂）模式。如果没有设置成 **non-silent** 模式，则默认假设端口处于沉寂（silent）状态。Silent 设置用于文件服务器或者包分析器。这种设置允许 PAgP 协议运行，把端口添加到通道组中，并且使用这个端口进行传输。 • **active**：仅当检测到一个 LACP 设备时才启用 LACP 模式。它把端口置于主动协商状态，端口通过发送 LACP 包与其他端口进行主动协商。 • **passive**：在端口上启用 LACP 模式，并且把端口置于被动协商状态，响应接收到的 LACP 包，但不会发送 LACP 包与其他端口进行协商
5	Switch(config-if)#**end**	返回到特权模式
6	Switch#**show running-config**	（可选）校验以上设置
7	Switch#**copy running-config startup-config**	（可选）保存配置到启动配置文件中

要从以太网通道中删除一个端口，可以使用 **no channel-group** 接口配置命令。

以下示例显示了如何在 Catalyst 3750 系列交换机堆叠的单一交换机上配置以太网通道。示例中以 PAgP desirable 模式分配 VLAN 10 中的两个静态访问端口（假设为 Catalyst 3750 的 1～2 号千兆端口）到通道 5 中。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable non-silent
Switch(config-if-range)# end
```

以下示例显示了如何在 Catalyst 3750 系列交换机堆叠的单一交换机上配置以太网通道。示例中以 LACP active 模式分配 VLAN 10 中的两个静态访问端口（假设为 Catalyst 3750 的 1~2 号千兆端口）到通道 5 中。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

以下示例显示了如何在 Catalyst 3750 系列交换机堆叠的单一交换机上配置以太网通道。示例中以 LACP passive 模式分配作为 VLAN 10 中堆叠成员 2 中的两个静态访问端口（假设为 Catalyst 3750 的 4～5 号千兆端口）和堆叠成员 3 中的一个静态访问端口（假设为 Catalyst 3750 的 3 号千兆端口）到通道 5 中。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/4 -5
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# exit
Switch(config)# interface gigabitethernet3/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# channel-group 5 mode active
Switch(config-if)# exit
```

5.3.4 配置三层以太网通道

在三层以太网通道配置方面，不同的 Catalyst 交换机系列中，具体的配置步骤有所不同。主要是以 Catalyst 3750 系列为分界线，在该系列以前（包括该系列）要配置三层太网通道，需要创建端口通道逻辑接口，然后把以太网端口添加到这个端口通道中；而在这个系列以后（不包括该系列）则没有分两步进行，只需在一个过程中完成。

1．在 Catalyst 3750 及以前系列中创建端口通道逻辑接口

在 Catalyst 3750 及以前系列中配置三层以太网通道时，应当首先通过使用 **interface port-channel** 全局配置命令手动创建这个端口通道逻辑接口，然后通过使用 **channel-group** 接口配置命令把逻辑接口添加到通道组中。

【注意】要从一个物理端口移动一个 IP 地址到以太网通道，则必须在配置端口通道接口以前从物理端口中删除这个 IP 地址。

按照表 5-8 所示的步骤为三层以太网通道创建一个端口通道接口（自特权模式开始）。

表 5-8 在 Catalyst 3750 及以前系列中创建三层以太网通道的步骤

步骤	命令	用途说明
1	Switch#**configure terminal**	进入全局配置模式
2	Switch(config)#**interface port-channel** *port-channel-number*	指定端口通道逻辑接口，并进入接口配置模式。 参数 *port-channel-number* 用于指定要创建的逻辑通道接口的通道号，范围是 1～48（此处是针对 Catalyst 3750 及早期其他系列交换机而言的，如果是像 Catlyst 6500 等中高档交换机系列，则可以最多创建 128 个以太网通道，具体参见相应产品说明书）。
3	Switch(config-if)#**no switchport**	把端口转换成三层模式
4	Switch(config-if)#**ip address** *ip-address mask*	为以太网通道分配 IP 地址和子网掩码
5	Switch(config-if)#**end**	返回到特权模式
6	**show etherchannel** *channel-group-number* **detail**	校验以上设置
7	Switch#**copy running-config startup-config**	（可选）在启动配置文件中保存设置
8		分配以太网端口到三层以太网通道中，具体将在本节后面的“配置物理接口”部分介绍

要删除端口通道，可以使用 **no interface port-channel** *port-channel-number* 全局配置命令。

以下示例显示了如何创建逻辑端口通道 5，并分配 IP 地址为 172.10.20.10。

```
Switch# configure terminal
Switch(config)# interface port-channel 5
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.10.20.10 255.255.255.0
Switch(config-if)# end
```

2．在 Catalyst 3750 及以前系列中配置物理接口

按照表 5-9 所示的步骤分配在 Catalyst 3750 及以前系列中的以太网端口到三层以太网通道中（自特权模式开始）。

表 5-9 在 Catalyst 3750 及以前系列中分配以太网端口到三层以太网通道的步骤

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*	指定要添加到以太网通道的一个物理端口，并进入接口配置模式。 对于 PAgP 模式以太网通道可以最多配置 8 个相同类型、相同速率的端口到同一个以太网通道中。 对于 LACP 模式以太网通道可以最多配置 16 个相同类型、相同速率的端口到同一个以太网通道中。其中最多 8 个处于活动状态，其他的为待机状态

续表

步骤	命令	用途说明
3	Switch(config-if)#**no ip address**	确保没有为接口分配 IP 地址
4	Switch(config-if)#**no switchport**	把端口转换成三层模式
5	Switch(config-if)#**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on**} | {**active** | **passive**}	分配端口到通道组，并且指定是工作于 PAgP 模式还是 LACP 模式。 参数 *channel-group-number* 用来指定通道组号，范围是 1～48（此处是针对 Catalyst 3750 及早期其他系列交换机而言的，如果是像 Catlyst 6500 等中高档交换机系列，则可以最多创建 128 个以太网通道，具体参见相应产品说明书）。 **mode** 关键字中的可选项说明如下： ● **auto**：仅当检测到一个 PAgP 设备时启用 PAgP。它将把端口置于被动协商状态，对所接收到的 PAgP 包进行响应，但不会发送 PAgP 包进行协商。该可选项在以太网通道成员来自交换机堆叠中的不同交换机时不支持。 ● **desirable**：无条件地启用 PAgP 模式。它将把端口置于主动协商状态。该端口会主动发送 PAgP 包与其他端口进行协商。该可选项在以太网通道成员来自交换机堆叠中的不同交换机时也不支持。 ● **on**：强迫通道中的端口不启用 PAgP 或者 LACP 协议。在 **on** 模式下，仅当一个 **on** 模式端口组与另一个 **on** 模式端口组连接时，才可能形成以太网通道。 ● **non-silent**：（可选）如果你的交换机是与一个支持 PAgP 协议的交换机连接，则配置这个交换机端口为 **non-silent**（非沉寂）模式。如果没有设置成 **non-silent** 模式，则默认假设端口处于沉寂（silent）状态。Silent 设置用于文件服务器或者包分析器。这种设置允许 PAgP 协议运行，把端口添加到通道组中，并且使用这个端口进行传输。 ● **active**：仅当检测到一个 LACP 设备时才启用 LACP 模式。它把端口置于主动协商状态，端口通过发送 LACP 包与其他端口进行主动协商。 ● **passive**：在端口上启用 LACP 模式，并且把端口置于被动协商状态，响应接收到的 LACP 包，但不会发送 LACP 包与其他端口进行协商
6	Switch(config-if)#**end**	返回到特权模式
7	Switch#**show running-config**	校验以上设置
8	Switch#**copy running-config startup-config**	（可选）在交换机启动配置文件中保存设置

以下示例显示了如何配置一个三层以太网通道。示例中是以 LACP active 模式分配两个端口（假设为 Catalyst 3750 型号堆叠成员 2 的 1～2 号千兆端口）到通道 5 中。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/1 -2
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

以下示例显示了如何配置三层以太网通道。示例中是以 LACP active 模式分配堆叠成员 2 中的两个端口（假设为 Catalyst 3750 的 4～5 号千兆端口）和堆叠成员 3 的一个端口（假设为 Catalyst 3750 的 3 号千兆端口）到 7 口中。

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/4 -5
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 7 mode active
Switch(config-if-range)# exit
Switch(config)# interface gigabitethernet3/0/3
Switch(config-if)# no ip address
Switch(config-if)# no switchport
Switch(config-if)# channel-group 7 mode active
Switch(config-if)# exit
```

3．把 Catalyst 4000 及以后系列物理接口配置为三层以太网通道

在 Catalyst 4000 及以后系列中，配置物理接口作为以太网通道端口成员的方法要简单一些，可以在一个过程中完成，但总体配置思路还是与以前系列类似，具体如表 5-10 所示。

表 5-10　配置物理接口为三层以太网通道的步骤

步骤	命令	用途说明
1	Switch#**configure terminal**	进入全局配置模式
1	Switch(config)#**interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port*	选择要配置的物理接口，并进入接口配置模式
2	Switch(config-if)#**no switchport**	把物理接口转成三层路由端口
3	Switch(config-if)#**no ip address**	确保该物理接口上没有分配 IP 地址
4	Switch(config-if)#**channel-group** *port_channel_number* **mode** {**active** | **on** | **auto** | **passive** | **desirable**}	配置端口通道中的接口，并指定采用 PAgP 模式还是 LACP 汇聚模式。 如果采用 PAgP 模式，则键入 **auto** 或者 **desirable** 关键字；如果采用 LACP 模式，则键入 **active** 或者 **passive** 关键字。 有关这些关键字的具体功能参见表 5-5
5	Switch(config-if)#**end**	退出接口配置模式，返回到特权模式
6	Switch#**show running-config interface port-channel** *port_channel_number* Switch#**show running-config interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* Switch#**show interfaces** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* **etherchannel** Switch#**show etherchannel 1 port-channel**	校验以上配置

以下示例显示了如何配置 Catalyst 4500 系列交换机的 Fast Ethernet interfaces 5/4 和 Fast Ethernet interfaces 5/5 这两个端口作为 PAgP **desirable** 模式端口通道成员。

```
Switch# configure terminal
Switch(config)# interface range fastethernet 5/4 - 5
Switch(config-if)# no switchport
Switch(config-if)# no ip address
Switch(config-if)# channel-group 1 mode desirable
Switch(config-if)# end
```

以下示例显示了如何校验上一示例中 Catalyst 4500 系列交换机 Fast Ethernet interface 5/4 端口的配置。

```
Switch# show running-config interface fastethernet 5/4
Building configuration...

Current configuration:
!
interface FastEthernet5/4
 no ip address
 no switchport
 no ip directed-broadcast
  channel-group 1 mode desirable
end

Switch# show interfaces fastethernet 5/4 etherchannel
Port state      = EC-Enbld Up In-Bndl Usr-Config
Channel group = 1              Mode = Desirable        Gcchange = 0
Port-channel   = Po1           GC     = 0x00010001     Pseudo-port-channel = Po1
Port indx       = 0            Load = 0x55

Flags:   S - Device is sending Slow hello.   C - Device is in Consistent state.
         A - Device is in Auto mode.         P - Device learns on physical port.
Timers: H - Hello timer is running.          Q - Quit timer is running.
         S - Switching timer is running.     I - Interface timer is running.

Local information:
                                    Hello     Partner  PAgP       Learning  Group
Port        Flags State     Timers  Interval  Count    Priority   Method    Ifindex
Fa5/4       SC      U6/S7           30s       1        128        Any       55
```

```
Partner's information:

                Partner                 Partner              Partner          Partner Group
Port        Name                        Device ID            Port        Age  Flags    Cap.
Fa5/4       JAB031301                   0050.0f10.230c       2/45          1s SAC       2D

Age of the port in the current state: 00h:54m:52s

Switch#
```

以下示例显示了如何校验 Catalyst 4500 系列交换机的端口通道 1 的配置。

```
Switch# show etherchannel 1 port-channel

                Channel-group listing:
                ----------------------
Group: 1
------------

                Port-channels in the group:
                ----------------------
Port-channel: Po1
------------

Age of the Port-channel   = 01h:56m:20s
Logical slot/port   = 10/1              Number of ports = 2
GC                  = 0x00010001        HotStandBy port = null
Port state          = Port-channel L3-Ag Ag-Inuse

Ports in the Port-channel:

Index   Load   Port
-------------------
  1      00    Fa5/6
  0      00    Fa5/7

Time since last port bundled:      00h:23m:33s      Fa5/6

Switch#
```

5.3.5　配置以太网通道负载均衡

本节将介绍如何配置以太网通道中各端口的负载均衡，这是以太网通道的一个主要应用。可以按照表 5-11 所示的步骤自特权模式开始配置以太网通道负载均衡（注意其中的不同系列配置命令）。

表 5-11　配置以太网通道负载均衡的步骤

步骤	命令	用途说明
1	Switch#**configure terminal**	进入全局配置模式
2	Catalyst 3750 及以前系列：Switch(config)# **port-channel load-balance** {**dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac**} Catalyst 4000 及以后系列：Switch(config)# **port-channel load-balance** {**src-mac** | **dst-mac** | **src-dst-mac** | **src-ip** | **dst-ip** | **src-dst-ip** | **src-port** | **dst-port** | **src-dst-port**}	配置以太网通道负载均衡方法，默认为 **src-mac**（源 MAC 地址）。具体方法解释如下： **dst-ip**：基于流入包的目标主机 IP 地址进行负载均衡 **dst-mac**：基于流入包的目标主机 MAC 地址进行负载均衡 **src-dst-ip**：基于流入包的源和目的主机 IP 地址进行负载均衡 **src-dst-mac**：基于流入包的源和目的主机 MAC 地址进行负载均衡 **src-ip**：基于流入包的源主机 IP 地址进行负载均衡 **src-mac**：基于流入包的源主机 MAC 地址进行负载均衡 如果是 Catalyst 4000 系列以后的交换机，则还支持起于源和目的 OSI/RM 第 4 层的端口进行均衡和数据转发的： ● src-port：源四层端口 ● dst-port：目的四层端口 ● src-dst-port：源和目的四层端口
3	Switch(config)# **end**	返回到特权模式
4	Switch# **show etherchannel load-balance**	校验以上设置
5	Switch# **copy running-config startup-config**	（可选）在交换机启动配置文件中保存以上设置

要恢复以太网通道负载均衡到默认设置，可以使用 **no port-channel load-balance** 全局配置命令。

以下示例显示了如何使用源和目的 IP 地址来配置以太网通道。

```
Switch# configure terminal
Switch(config)# port-channel load-balance src-dst-ip
Switch(config)# end
Switch#
```

以下示例显示了如何校验上一示例中的以太网通道配置。

```
Switch# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
        src-dst-ip

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
  IPv4: Source XOR Destination IP address
  IPv6: Source XOR Destination IP address
Switch#
```


5.3.6 从以太网通道中删除接口

如果觉得某个原来在以太网通道中的接口不需要或者该端口有其他用途了，则可以从以太网通道中删除该接口，方法如表 5-12 所示。

表 5-12 从以太网通道中删除接口的步骤

步骤	命令	用途说明
1	Switch(config)# **interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port*	选择要删除的接口，并进入接口配置模式
2	Switch(config-if)# **no channel-group**	从端口通道接口中删除上述接口
3	Switch(config-if)# **end**	退出接口配置模式
4	Switch# **show running-config interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* Switch# **show interface** {**fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* **etherchannel**	校验以上配置

以下示例显示了如何从端口通道 1 中删除 Fast thernet interfaces 5/4 和 5/5 这两个接口。

```
Switch# configure terminal
Switch(config)# interface range fastethernet 5/4 - 5 (Note: Space is mandatory.)
Switch(config-if)# no channel-group 1
Switch(config-if)# end
```

5.3.7 删除以太网通道

如果不再需要某个以前配置的以太网通道，则也可以删除，释放通道端口中的接口，用于独立通信。删除以太网通道后，通道中的端口将关闭并且从通道组接口中删除，具体步骤如表 5-13 所示。

表 5-13 删除以太网通道的步骤

步骤	命令	用途说明
1	Switch(config)# **no interface port-channel** *port_channel_number*	删除端口通道接口
2	Switch(config)# **end**	退出全局配置模式
3	Switch# **show etherchannel summary**	校验以上配置

【注意】如果要把二层以太网通道转换成三层以太网通道，或者把三层以太网通道转换成二层以太网通道，则必须删除以太网通道，然后在 **PAgP desired** 配置中重建相应类型的通道。

以下示例显示了如何删除端口通道 1。

```
Switch# configure terminal
Switch(config)# no interface port-channel 1
Switch(config)# end
```

5.4　配置 SNMP

SNMP（Simple Network Management Protocol，简单网络管理协议）是专门设计用来在 IP 网络管理网络节点（服务器、工作站、路由器、交换机等）的一种标准应用层协议。SNMP 是通过 UDP 协议工作的，所以其中的消息格式都是以 UDP 数据报格式封装的。通过 SNMP 协议，可以在一个站点管理网络中所有支持该协议的设备。本节要介绍如何在 Cisco Catalyst 以太网交换机（如 Catalyst 3550/3750/4500/6500 等系列）中配置和使用 SNMP 管理网络设备。

5.4.1　理解 SNMP

SNMP 管理系统包含一个 SNMP 管理器（安装了 SNMP 管理应用程序的站点）、一个 SNMP 代理和一个 MIB（Management Information Base，管理信息库）。SNMP 管理器可以是安装了像 CiscoWorks 这样的站点，SNMP 代理和 MIB 都是位于交换机内部的。它们三者之间的关系可以用图 5-8 表示。这样来看，本节后面介绍的 SNMP 配置也只是针对交换机上的 SNMP 代理和 MIB 而言，并不是直接配置 SNMP 管理器的，因为 SNMP 管理器不是交换机。当然，在交换机上配置 SNMP 代理、MIB 时，必须定义 SNMP 管理器与 SNMP 代理之间的关系。

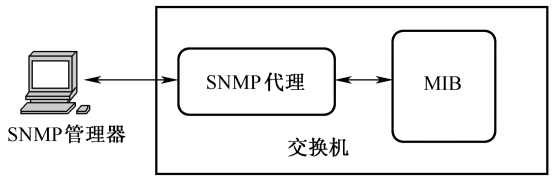

图 5-8　SNMP 管理系统结构

SNMP 代理包含 SNMP 管理器可以请求和修改的 MIB 变量。SNMP 管理器可以从 SNMP 代理那里得到变量的值，也可以把修改后的变量值存储在 SNMP 代理中。SNMP 代理收集从 MIB 中得到的数据、有关设备参数的信息库和网络数据。SNMP 代理也可响应 SNMP 管理器的请求，以获取或者设置数据。

SNMP 代理可以主动发送 Trap 通知到 SNMP 管理器（Trap 是 SNMP 管理器发送的网络情形的警报消息）。Trap 消息通常意味着有异常用户认证、重新启动、链路状态启用或关闭、MAC 地址寻址、一个 TCP 连接关闭、邻居连接丢失，或者其他重要事件发生。当然，也可以不用 SNMP 代理，让 SNMP 管理器直接与 MIB 进行联系，毕竟它是 SNMP 管理器与 MIB 之间请求和消息发送的代理，具体配置方法将在本节后面详细介绍。

1．SNMP 版本

目前，SNMP 有 3 种主要版本：SNMPv1、SNMPv2、SNMPv3。v1 和 v2 没有太大差别，但 SNMPv2 是增强版本，包含了其他协议操作。与前两个版本相比，SNMPv3 则包含更多安全和远程配置。为了解决不同 SNMP 版本间的不兼容问题，RFC 3584 文档中定义了三者共存策略。下面介绍的是在 Catalyst 3750/4500 及以后交换机中支持的 SNMP 版本：

- SNMP v1：SNMP 的最初正式应用完整互联网标准版本，在 RFC 1157 中定义。
- SNMPv2C 家族：以基于公共字符串（community-string-based）的 SNMPv2C 管理架构取代基于参与（Party-based）管理模式的 SNMPv2 家族安全架构，同时保留整体检索，并改进了 SNMPv2 家族中的错误处理方式。它包含以下子版本：
  - SNMPv2：SNMP 的第二个版本，是一个互联网标准的草案版本，在 RFC 1902～1907 中定义。

- SNMPv2C：基于公共字符串管理架构的 SNMPv2，是一个修订的互联网协议，在 RFC 1901 中定义。

- SNMPv3：SNMPv3 是一个能协商操作的版本，在 RFC 2273～2275 中定义。SNMPv3 通过身份认证和加密数据包来提供在网络中对设备的安全访问。它包括以下特性：
  - 消息完整性检查：确保消息数据包在传送过程中没有被破坏。
  - 身份认证：确保消息是来自合法的源。
  - 加密：重新混合消息包的内容，以阻止未授权的源读取包中的内容。

SNMPv1 和 SNMPv2C 使用公共字符串安全架构。SNMP 管理器公共组成员可以通过 IP 地址访问控制列表和密码访问 SNMP 代理所定义的 MIB。

SNMPv2C 包括一个整体检索机制，并可为管理器提供更详细的错误消息报告。整体检索机制可以检索表格和大量的信息，减少了需要往返传送的消息数量。SNMPv2C 改进了 SNMPv1 的错误处理方式，包括扩展了用于区别不同类型错误事件的错误代码。这些事件在 SNMPv1 中是以单一错误代码提供报告的，而在 SNMPv2C 的出错返回报告中报告了错误类型。

SNMPv3 提供了安全模式（Security Model）和安全级别（Security Level）。安全模式是一个用户和组的身份认证策略；安全级别是在安全模式中的安全许可级别。一个安全级别和安全模式的组合决定了在处理 SNMP 数据包时采用哪个安全机制。可用的安全模式有：SNMPv1、SNMPv2C 和 SNMPv3。

不同安全级别和安全模式组合的特性如表 5-14 所示。

表 5-14　SNMP 安全模式和级别

模式	级别	身份认证	加密	结果
SNMPv1	noAuthNoPriv	Community string（公共字符串）	无	在身份认证中使用一个公共字符串来进行匹配
SNMPv2C	noAuthNoPriv	Community string（公共字符串）	无	在身份认证中使用一个公共字符串来进行匹配
SNMPv3	noAuthNoPriv	Username（用户名）	无	在身份认证中使用一个用户名来匹配
SNMPv3	authNoPriv	MD5 或者 SHA	无	提供基于 HMAC-MD5 或者 HMAC-SHA 算法的身份认证
SNMPv3	AuthPriv（需要加密软件映象）	MD5 或者 SHA	DES	提供基于 HMAC-MD5 或者 HMAC-SHA 算法的身份认证。在基于 CBC-DES（DES 56）身份认证标准基础上提供 DES 56 位数据加密

必须配置 SNMP 代理来使用管理器支持的 SNMP 版本。因为一个 SNMP 代理可以与多个 SNMP 管理器通信，所以可以配置软件支持使用 SNMPv1、SNMPv2C 和 SNMPv3 版本协议。

2．SNMP 管理器功能

SNMP 管理就是安装了 SNMP 管理应用程序的站点，与安装了其他服务器软件的站点具有一定管理功能一样，SNMP 管理器的作用就是用于管理网络中的设备。SNMP 管理器使用在 MIB 中的信息来完成表 5-15 所示的操作。

表 5-15　SNMP 操作

操作	描述
get-request	从指定的变量中检索变量值
get-next-request	从一个表内的一个变量中检索变量值，SNMP 管理器并不需要知道确切的变量名，而是在表格中按照顺序检索的方式查找所需的变量的
get-bulk-request2	检索大数据块，如一个表内的多行，或者需要传送多个小数据块。仅在 SNMPv2 及以后版本中支持
get-response	通过 NMS 为 get-request、get-next-request 和 set-request 发送应答
set-request	在指定变量中存储值
trap	在发生一些事件后，通过 SNMP 代理发送到 SNMP 管理器的主动消息

3．SNMP 代理功能

交换机上的 SNMP 代理具体负责代理 SNMP 管理器的以下请求：

- 获取 MIB 变量：SNMP 代理检索被 SNMP 管理器请求的 MIB 变量，并以检索到的变量值响应 SNMP 管理器中的 NMS（网络管理系统）。
- 设置 MIB 变量：SNMP 代理在响应 NMS 消息中提供这一功能。SNMP 代理改变由 NMS 请求的 MIB 变量值。

SNMP 代理也会主动发送 trap 触发消息，以通知 NMS 在 SNMP 代理上所发生的重要事件。包括但不限于以下事件：端口/模块打开或者关闭了、生成树拓扑结构发生了改变、身份认证失败等。

4．SNMP 公共字符串

SNMP 公共字符串（Community String）是一个起着密码作用的文本串，其被用来鉴别在管理器站点和一个包含 SNMP 信息的 SNMP 代理之间的信息发送。这个公共字符串被发送到在管理器和代理之间的每个数据包，是以嵌入密码方式验证对 MIB 对象和功能的访问。

公共字符串可以具有以下属性之一：

- 只读（Read-only，RO）：具有以只读方式访问授权的管理器以及在 MIB 中的所有对象，除了公共字符串外，但是不允许进行写入操作。
- 读写（Read-write，RW）：具有以读写方式访问授权的管理器以及在 MIB 中的所有对象，但是不允许访问公共字符串。
- 全部读写（Read-write-all）：具有以读写方式访问授权的管理器以及在 MIB 中的所有对象，包括公共字符串。

5．使用 SNMP 访问 MIB 变量

CiscoWorks 网络管理软件是 NMS 的一个示例，使用交换机 MIB 变量来设置设备变量，并为指定信息轮询网络中的设备。轮询的结果可以以图形方式显示。它可以为排除网络故障提供分析，并可提高网络性能，校验设备配置，监控流量负载等。

在图 5-9 中，SNMP 代理从 MIB 中搜集数据，然后在需要时，SNMP 代理可以发送 trap 触发或者事件通知到 SNMP 管理器。也就是说，一般情况下，SNMP 管理器是不会直接与 MIB 联系，从 MIB 中搜集数据的，而是直接从 SNMP 代理中获得变量值，则 SNMP 代理从 MIB 中搜集变量数据，并保存在 SNMP 代理内存中。

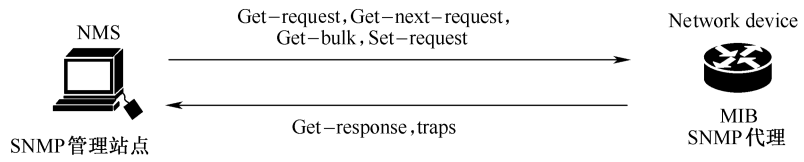

图 5-9　SNMP 网络示例

SNMP 代理所发送的 Trap 用于提醒 SNMP 管理器发生了某种事件，如禁止用户身份认证、重新启动、链路启用或关闭、MAC 地址跟踪等。SNMP 代理也可以 *get-request*、*get-next-request* 和 *set-request* 消息格式（消息解释参见表 5-17）响应由 SNMP 管理器发送的相关 MIB 查询。

6．SNMP 通知

SNMP 允许交换机在发生特定事件时通过 SNMP 代理发送通知到 SNMP 管理器。SNMP 通知可以作为 trap 或者通告（Inform）请求这两种方式发送。在使用 **snmp-server host** 命令指定接收 SNMP 通知的网络设备时，如果有选择 **traps** 或者 **informs** 选项，则表示指定要么以 Trap 方式发送 SNMP 通知，要么以 Inform 方式向 SNMP 管理器发送 SNMP 通知。

【注意】SNMPv1 不支持通告。

Trap 是一种随机触发的不可靠的消息发送方式，因为接收者在接收到 Trap 后不会发送确认消

息，这样发送者就不能确定 Trap 是否已发送。当一个 SNMP 管理器接收到一个 Inform 请求时，它将以一个 SNMP 响应协议数据单元（Protocol Data Unit，PDU）来发送一个响应消息。如果发送者没有接收到响应，则 Inform 请求可以重新发送。因为可以重新发送，而且可以接收响应消息，所以 Inform 与 Trap 相比，更适用于有明确目标的情形。

这一特性使得 Inform 比 Trap 更具有可用性，但同时也要消耗交换机和网络的更多资源。因为不像 Trap 发送后立即丢弃，Inform 请求会在内存中保存，除非接收到了响应或者请求发送超时。而且 Trap 请求只发送一次，但是 Inform 请求可以重发或者重试多次。重试会增加网络通信流量，消耗更多的网络资源。所以，Trap 和 Inform 方式的选择需要在可用性和资源方面做权衡选择。如果想要 SNMP 管理器接收每一个通知，则建议使用 Inform 请求方式；如果更关心网络或者内存资源的利用率，则选择使用 Trap。

5.4.2 Catalyst 交换机上的 SNMP 默认配置

与其他功能一样，交换机上的 SNMP 功能也有其默认属性配置。了解这些默认配置有助于手动改变相应属性配置。表 5-16 所示为 Catalyst 交换机的默认 SNMP 配置。

表 5-16 默认 SNMP 配置

特征	默认设置
SNMP agent	Enabled
SNMP trap 接收器	没有配置
SNMP traps	除了 TCP 连接的 Trap 外，其他没有启用
SNMP version	如果没有配置 **version** 关键字，默认是版本 1
SNMPv3 authentication	如果没有键入关键字，默认是 **noauth**（noAuthNoPriv）安全级别
SNMP notification type	如果没有指定类型，则通告都将被发送

5.4.3 SNMP 配置指南

一个 SNMP 组（Group）是一个映射 SNMP 用户（其实通俗点讲就是使用 SNMP 协议、被管理的网络设备）到 SNMP 视图的表。视图表中的 SNMP 用户（User）是 SNMP 组的成员；SNMP 主机（host，其实就是 SNMP 管理器）是 SNMP Trap 的接收者；SNMP 引擎 ID（Engine ID）是本地或者远程 SNMP 引擎名称（SNMP 引擎是位于 SNMP 管理器中的程序）。

在配置 SNMP 时，建议参考以下指南：

- 在配置 SNMP 组时，不要指定通知视图。因为 **snmp-server host** 全局配置命令会为用户自动协商通知视图，并添加到与用户协商的组中。编辑组通知视图会影响所有与组关联的用户。
- 要配置远程用户，指定用户所处的远程设备的 SNMP 代理的 IP 地址或者端口号。
- 在为特定代理配置远程用户时，请使用 **snmp-server engineID** 全局配置命令的 **remote** 选项来配置 SNMP 引擎 ID。远程代理的 SNMP 引擎 ID 和用户密码用于计算身份认证和加密摘要。如果先不配置远程引擎 ID，则配置命令会无效。
- 在配置 SNMP 通知时，在可以发送代理请求或者通知前，需要为 SNMP 数据库中的远程代理配置 SNMP 引擎 ID。
- 如果本地用户没有与远程主机关联，交换机不能以 **auth**（authNoPriv）和 **priv**（authPriv）认证级别发送通告。
- 改变 SNMP 引擎 ID 有很大的负面影响。在命令行中键入的用户密码是基于用户密码本身和本地引擎 ID 来转换成 MD5 或者 SHA 安全摘要的，然后命令行输入的密码会被销毁。正是这个原因，引擎 ID 改变后，SNMPv3 的安全摘要用户就会变成无效，需要重新通过

snmp-server user *username* 全局配置命令配置 SNMP 用户。同样，对于公共字符串在引擎 ID 发生改变后也需要重新配置。

5.4.4　禁用 SNMP 代理

SNMP 代理不是管理应用程序，只是一个接口程序。SNMP 管理应用程序（SNMP 管理器）通过它请求检索数据和设置管理属性。SNMP 代理使用 UDP 协议与 SNMP 管理应用程序通信。UDP 协议还允许 SNMP 代理和 SNMP 管理应用程序驻留在同一台机器上或不同的机器上。当然也可以不要 SNMP 代理，这主要是出于安全考虑，因为使用 SNMP 代理容易出现一些远程拒绝服务攻击。

如果要在交换机上禁用 SNMP 代理，请按表 5-17 所示的步骤进行。

表 5-17　禁用 SNMP 代理的步骤

步骤	命令	用途说明
1	Switch# **configure terminal**	进入全局配置模式
2	Switch(config)# **no snmp-server**	禁用 SNMP 代理运行
3	Switch(config)# **end**	返回到特权模式
4	Switch# **show running-config**	校验以上设置
5	Switch# **copy running-config startup-config**	（可选）把以上配置保存在当前运行配置文件中

执行 **no snmp-server** 全局配置命令会禁用设备上运行的所有 SNMP 版本，包括 SNMPv1、SNMPv2C 和 SNMPv3。而且要注意的是，没有指定 IOS 命令来启用 SNMP。但在一开始所键入的 **snmp-server** 全局配置命令会启用所有 SNMP 版本。

5.4.5　配置公共字符串

可以使用 SNMP 公共字符串（Community String）来定义 SNMP 管理器和 SNMP 代理之间的关系。公共字符串就像密码一样来限定访问交换机上的 SNMP 代理，只有配置了正确的公共字符串才可以访问来自 SNMP 代理程序的信息。公共字符串的字符串长度不能大于 64 个字符。也可以用字符串来指定以下一个或者多个这样的特性：

- 允许使用公共字符串来获取访问 SNMP 代理的 SNMP 管理器的 IP 地址访问列表。
- MIB 视图，定义可以访问给定公共字符串的所有 MIB 对象子网。
- 读取和写入，或者仅读取 MIB 对象访问公共字符串的权限。

在交换机上配置公共字符串的步骤如表 5-18 所示。

表 5-18　在交换机上配置公共字符串的步骤

步骤	命令	用途说明
1	Switch# **configure terminal**	进入全局配置模式
2	Switch(config)# [**no**] **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [*access-list-number*]	配置公共字符串。 *string* 参数指定一个像密码一样的字符串，以限制访问 SNMP 代理。可以配置一个或者多个公共字符串，最多 117 个字符。 （可选）**view** 关键字指定可以访问公共字符串的视图记录，后面的 *view-name* 参数是指定视图名称。 （可选）如果要授权 SNMP 管理器检索 MIB 对象，则可以指定选择 **ro** 关键字选项；如果要授权 SNMP 管理器检索和编辑 MIB 对象，则要选择 **rw** 关键字选项。默认情况下，公共字符串允许以只读方式访问所有对象。 （可选）*access-list-number* 参数可用于键入一个 1～99 或者 1300～1999 的 IP 访问列表（ACL）号。有关 Cisco Catalyst 交换机的 ACL 方面的内容将在第 8 章介绍。 可以使用 **no snmp-server community** *string* 全局配置命令删除指定的公共字符串

续表

步骤	命令	用途说明
3	Switch(config)# **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	（可选）如果在上一步中指定了一个标准 IP ACL，可以根据需要多次使用本步所示的命令。 *access-list-number* 参数用于指定上一步中所指定的 ACL 号；**deny** 关键字用于指定在条件满足时拒绝访问；**permit** 关键字用于指定在条件满足时允许访问。 *source-wildcard* 参数是以十进制方式指定源设备的 IP 通配符掩码（wildcard），凡是要忽略的位置都是 1（其实就是 IP 地址的取反，即原来为 1 的位置 0，原来为 0 的位置 1 得到的）。有关通配符掩码将在第 8 章介绍 ACL 时具体介绍
4	Switch(config)# **end**	返回到特权模式
5	Switch# **show running-config**	校验以上设置
6	Switch# **copy running-config startup-config**	（可选）在当前运行配置文件中保存以上设置

以下示例显示了如何启用所有版本的 SNMP，并配置允许任何 SNMP 管理器通过公共字符串 *public* 以只读权限访问所有对象。

```
Switch(config)# snmp-server community public
```

要禁止访问 SNMP 公共字符串，可以设置公共字符串为空（也就是不键入公共字符串）。

【注意】不支持 snmp-server enable informs 命令。要启用 SNMP 通告消息发送，需要使用 **snmp-server enable traps** 和 **snmp-server host** *host-addr* **informs** 组合命令。

下面的示例显示了如何为 SNMP 代理指派公共字符串 *comaccess*，并允许以只读方式访问，指定可以使用公共字符串来访问交换机上的 SNMP 代理的 ACL 为 ACL 4。

```
Switch(config)# snmp-server community comaccess ro 4
```

5.4.6 SNMP 组和用户

可以为交换机上本地或者远程 SNMP 服务器引擎指定用于标识的引擎 ID（Engine ID）。也可以配置一个用于映射 SNMP 用户（被 SNMP 管理的设备）到 SNMP 视图的 SNMP 服务器组，然后添加新的用户到 SNMP 组中。在交换机上配置 SNMP 组和用户的步骤如表 5-19 所示。具体的综合配置示例在 5.4.10 节介绍。

表 5-19 在交换机上配置 SNMP 组和用户的步骤

步骤	命令	用途说明
1	Switch# **configure terminal**	进入全局配置模式
2	Switch(config)# **snmp-server engineID** {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}	为本地或者远程 SNMP 服务器副本配置引擎 ID。 参数 *engineid-string* 用于指定 SNMP 映射引擎名，24 个字符串 ID。如果有尾随 0，则可以不必输入 24 个字符。如引擎 ID 为 123400000000000000000000，则可直接键入 **snmp-server engineID local 1234**。 如果选择 **remote** 关键字，则可指定包含远程 SNMP 副本的设备的 IP 地址和远程设备上的可选 UDP 端口。默认的 UDP 端口为 162
3	Switch(config)# **snmp-server** | **note group** *groupname* {**v1** | **v2c** | **v3** [**auth** | **noauth** | **priv**]} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	在远程设备上配置新的 SNMP 组。 参数 *groupname* 用于指定组名。其中关键字 **v1**、**v2c** 和 **v3** 对应 SNMP 的 3 个版本，也可以说是对应 3 个不同的安全模式。关键字 **auth**、**noauth** 和 **priv** 对应 3 种不同的 SNMP 安全级别，参见表 5-14。 键入一个带有不超过 64 个字符的 **read** *readview* 参数来指定只有可以查看 SNMP 代理中内容的视图名称。 键入一个带有不超过 64 个字符的 **write** *writeview* 参数来指定可以键入数据，配置 SNMP 代理中内容的视图名称。 键入一个带有不超过 64 个字符的 **notify** *notifyview* 参数来指定可以编辑、通告或者 trap 的视图名称。 键入一个带有不超过 64 个字符的 **access** *access-list* 参数来指定访问列表名称

续表

步骤	命令	用途说明
4	Switch(config)# **snmp-server user** *username groupname* [**remote** *host* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**auth** {**md5** | **sha**} *auth-password*]} [**encrypted**] [**access** *access-list*]	为一个 SNMP 组添加用户。 参数 *username* 是连接到 SNMP 代理的主机用户名称。 参数 *groupname* 是与上述指定用户关联的组的名称。 参数 **remote** *host* [**udp-port** *port*]]用于指定一个上述指定用户所属的远程 SNMP 实体的主机名或者带有 UDP 端口的 IP 地址。端口号默认为 162。 **v1** | **v2c** | **v3** 关键字用于指定所使用的 SNMP 版本。如果键入 **v3**，则可以有如下可选项： 可选项 **auth** {**md5** | **sha**} *auth-password*]}是指定会话的身份认证级别，可以是 HMAC-MD5-96、HMAC-SHA-96 或者一个不超过 64 个字符的密码字符串。 可选项 **encrypted** 用于指定在加密格式中显示的密码。 可选项 **access** *access-list* 是一个不超过 64 个字符的访问列表名称
5	Switch(config)# **end**	返回到特权模式
6	Switch# **show running-config**	校验以上设置
7	Switch# **copy running-config startup-config**	（可选）在当前运行的配置文件中保存以上设置

5.4.7　配置 SNMP 通知

一个 trap 管理器就是一个接收和处理 trap 的 SNMP 管理器。trap 是由交换机在发生某种特定事件时所产生的系统警报。默认情况下，是没有定义 tarp SNMP 管理器的，也不会发送 trap 警报。运行 Cisco IOS 12.2(31)SG 版本的交换机可以有不受限制的 trap 管理器数量。

【说明】许多 SNMP 命令中使用 ***trap*** 关键字，除非在命令的选项中要选择 trap 或者 inform，否则关键字 *trap* 是指 trap 或者 inform，或者两者都可以。使用 **snmp-server host** 命令指定在发送 SNMP 通知时是采用 traps 还是采用 inform。

表 5-20 所示为 Cisco 交换机所支持的 trap 通知类型。可以启用任一或者所有这些 trap，并配置 trap 管理器来接收它们。

表 5-20　Cisco 交换机所支持的 trap 通知类型

trap 通知类型	描述
bgp	产生 BGP 状态改变 trap。本 trap 仅在安装了增强型多层映象时才可启用
bridge	产生 STP 桥接 MIB trap
config	为 SNMP 配置改变所产生的 trap
config-copy	为 SNMP 副本配置改变所产生的 trap
cpu	允许相关 CPU trap
eigrp	启用 BGP trap。本 trap 仅在安装了增强型多层映象时才可启用
entity	为 SNMP 实体改变所产生的 trap
envmon	产生环境监控 trap。可以启用任一或者所有这些环境 trap：fan（风扇）、shutdown（关闭）、supply（电源）和 temperature（温度）
flash	产生 SNMP Flash 通知
fru-ctrl	产生 SNMP 实体 FRU（Field Replaceable Unit，现场可换单元）控制 trap
hsrp	为 HSRP（Hot Standby Router Protocol，主机热备份路由器协议）更改所产生的 trap
ipmulticast	为 IP 多播路由改变所产生的 trap
isis	启用 IS-IS（Intermediate System to Intermediate System，中间系统到中间系统的路由选择协议）的 trap。本 trap 仅在安装了增强型多层映象时才可启用
mac-notification	为 MAC 地址通知所产生的 trap
msdp	为 MSDP（Multicast Source Discovery Protocol，多播资源发现协议）改变所产生的 trap。本 trap 仅在安装了增强型多层映象时才可启用
ospf	为 OSPF（Open Shortest Path First，开放最短路径优先）改变所产生的 trap。可以启用以下任一或者所有 trap：Cisco specific（Cisco 指定的）、errors（错误）、link-state advertisement（链路状态广告）、rate limit（速率限制）、retransmit（重传）和 state changes（状态改变）。 本 trap 仅在安装了增强型多层映象时才可启用

续表

trap 通知类型	描述
pim	为 PIM（Protocol-Independent Multicast，独立协议组播）改变所产生的 trap。可以启用以下任一或者所有 trap：invalid PIM messages（无效 PIM 消息）、neighbor changes（邻居改变）和 rendezvous point (RP)-mapping changes（会聚点映射改变）
port-security	产生 SNMP 端口安全 trap。也可以设置一个发送这种 trap 的最大速率，范围为 0～1000，默认为 0，表示不受限制，在发生 SNMP 端口安全时就发送这个 trap
rf	启用在 Cisco-RF-MIB 中定义的所有 SNMP trap
snmp	为 SNMP 类型身份认证、冷启动、热启动、链路启用或者关闭通知所产生的 trap
storm-control	为 SNMP 风暴控制所产生的 trap。也可以设置一个发送这种 trap 的最大速率，范围为 0～1000，默认为 0，表示不受限制，在发送风暴时就发送这个 trap
stpx	为 SNMP 扩展 STP（生成树协议）MIB 所产生的 trap
syslog	为 SNMP 系统日志所产生的 trap
tty	为 TCP 连接所产生的 trap。这种 trap 是默认启用的
vlan-membership	为 SNMP VLAN 成员改变所产生的 trap
vlancreate	为 SNMP VLAN 创建所产生的 trap
vlandelete	为 SNMP VLAN 删除所产生的 trap
vtp	为 VTP（VLAN Trunking Protocol，VLAN 中继协议）改变所产生的 trap

可以使用 **snmp-server host** 全局配置命令来指定主机（也就是 SNMP 管理器站点）接收表 5-20 中所列的 trap 通知类型。当然 SNMP 通知还可以是前面介绍的 inform 方式。配置交换机发送 trap 或者 inform 通知到主机的步骤如表 5-21 所示。具体的综合配置示例在 5.4.10 节介绍。

表 5-21　配置交换机发送 trap 或者 inform 通知到主机的步骤

步骤	命令	用途说明
1	Switch# **configure terminal**	进入全局配置模式
2	Switch(config)# **snmp-server engineID remote** *ip-address engineid-string*	指定远程主机的引擎 ID
3	Switch(config)# **snmp-server user** *username groupname* **remote** *host* [**udp-port** *port*] {**v1** | **v2c** | **v3** [**auth** {**md5** | **sha**} *auth-password*]} [**encrypted**] [**access** *access-list*]	配置与第 2 步中指定的远程主机相关联的 SNMP 用户。如果事先没有配置远程主机的引擎 ID，则不能配置远程用户。如果试图在配置远程主机引擎 ID 前配置 SNMP 用户，你将接收到一个错误消息，命令不会执行。 *username groupname* 参数用于指定 SNMP 用户的用户名和所属组名 **remote** *host* [**udp-port** *port*]参数用来指定上一步所定义的远程主机名，或者再指定所用的 UDP 端口号（默认为 162） **v1** | **v2c** | **v3** 关键字用于指定所使用的 SNMP 版本。如果键入 **v3**，则可以有如下可选项： **auth** {**md5** | **sha**} *auth-password*]}是指定会话的身份认证级别，可以是 HMAC-MD5-96、HMAC-SHA-96 或者一个不超过 64 个字符的密码字符串。 可选项 **encrypted** 用于指定在加密格式中显示的密码。 可选项 **access** *access-list* 是一个不超过 64 个字符的访问列表名称
4	Switch(config)# **snmp-server host** *host-addr* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]	指定 SNMP trap 选项的接受者。 参数 *host-addr* 用于指定主机（目标接受者）的名称或者 IP 地址。 选择 **traps** 关键字来发送 SNMP trap 到目标主机。 选择 **informs** 关键字来发送 SNMP inform 到目标主机。 参数 **version** {**1** | **2c** | **3** 是用来指定所使用的 SNMP 版本。如果选择了版本 3，则可以使用后面的[**auth** | **noauth** | **priv**]}可选项，用于选择身份认证级别，参见表 5-14。选择 **priv** 安全级别时，仅在安装了加密软件映射时才可用。 参数 *community-string* 用于指定在通知发送操作中所使用的像密码一样的公共字符串。 **udp-port** *port* 可选项用于指定 SNMP 远程设备所使用的 UDP 端口。 *notification-typ* 可选项使用表 5-15 中所指定的 trap 通知类型。如果没有指定，则所有通知都是可以发送的
5	Switch(config)# **snmp-server enable traps** *notification-types*	启用交换机发送 trap 或者 inform，或者所指定的 trap 类型的通知。要启用多个 trap 类型，必须为每个 trap 类型分别键入一个 **snmp-server enable traps** 命令

续表

步骤	命令	用途说明
6	Switch(config)# **snmp-server trap-source** *interface-id*	（可选）指定提供 trap 消息的源接口 IP 地址。这个命令也设置 inform 类型通知的源 IP 地址
7	Switch(config)# **snmp-server queue-length** *length*	（可选）为 trap 主机建立消息查询的长度，取值范围为 1～1000，默认为 10
8	Switch(config)# **snmp-server trap-timeout** *seconds*	（可选）定义重发 trap 消息的频率，取值范围为 1～1000 秒，默认为 30 秒
9	Switch(config)# **end**	返回到特权模式
10	Switch# **show running-config**	校验以上设置
11	Switch# **copy running-config startup-config**	（可选）在当前运行的配置文件中保存以上设置

snmp-server host 命令用于指定接收通知的主机；**snmp-server enable trap** 命令用于全局启用指定通知（包括 trap 和 inform）机制；要启用一个主机接收 inform 通知，必须为主机配置 **snmp-server host informs** 命令，并通过 **snmp-server enable traps** 命令全局启用 inform 通知类型。

要删除指定主机接收 trap 通知，可使用 **no snmp-server host** *host* 全局配置命令；**no snmp-server host** 命令用于禁用主机接收 trap 通知，但是不禁用主机接收 inform 通知。要禁用 inform 通知，可使用 **no snmp-server host informs** 全局配置命令；要禁用指定的 trap 类型，可使用 **no snmp-server enable traps** *notification-types* 全局配置命令。

5.4.8　限制通过 SNMP 使用 TFTP 服务器

要限制通过 SNMP 使用 TFFP 服务器保存和上传配置文件到访问列表中指定的服务器中，可按表 5-22 所示的配置步骤进行。具体的综合配置示例在 5.4.10 节介绍。

表 5-22　限制通过 SNMP 使用 TFFP 服务器保存和上传配置文件到访问列表中指定的服务器中的配置步骤

步骤	命令	用途说明
1	Switch# **configure terminal**	进入全局配置模式
2	Switch(config)# **snmp-server tftp-server-list** *access-list-number*	限制通过 SNMP 使用 TFFP 服务器复制配置文件到访问列表中指定的服务器。 参数 *access-list-number* 用于指定一个标准的 IP 访问列表号，取值范围为 1～99 或者 1300～1999
3	Switch(config)# **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	根据需要，创建所需个数的标准 IP 访问列表。 参数 *access-list-number* 是第 2 步所指定的访问列表号。 关键字 **deny** 用于在条件满足时禁止访问；关键字 **permit** 用于在条件满足时允许访问。 参数 *source-wildcard* 用于指定要应用的源通配符掩码。具体的通配符掩码参见第 8 章的相关内容
4	Switch(config)# **end**	返回到特权模式
5	Switch# **show running-config**	校验以上设置
6	Switch# **copy running-config startup-config**	（可选）在当前运行的配置文件中保存以上设置

5.4.9　SNMP 配置示例

以下示例显示了如何允许任何 SNMP 管理器以公共字符串访问 *public* 以只读权限访问所有对象。交换机使用 SNMPv1 发送 VTP trap 到 IP 地址为 192.180.1.111 和 192.180.1.33 的主机，以使用 SNMPv2C 发送 VTP trap 到 IP 地址为 192.180.1.27 的主机。公共字符串 *public* 是与 trap 一起发送的。

```
Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps vtp
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(config)# snmp-server host 192.180.1.33 public
```

以下示例显示了如何允许 ACL 4 中的成员以只读方式用公共字符串 *comaccess* 访问所有对象。禁止其他所有 SNMP 管理器访问任何对象。SNMP 身份认证失败 trap 是使用 SNMPv2C 以公共字符串 *public* 发送到 *cisco.com* 主机的。

```
Switch(config)# snmp-server community comaccess ro 4
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)# snmp-server host cisco.com version 2c public
```

以下示例显示了如何发送 Entity（实体）MIB trap 到 *cisco.com* 主机，不使用公共字符串。第 1 行启用交换机仅发送 Entity MIB trap，第 2 行是指定接收这些 trap 的目的主机为 *cisco.com*，并且重写以前在 **snmp-server host** 命令中所设置的主机。

```
Switch(config)# snmp-server enable traps entity
Switch(config)# snmp-server host cisco.com restricted entity
```

以下示例显示了如何使用公共字符串 *public* 启用交换机发送所有 trap 到 *myhost.cisco.com* 主机上。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

以下示例显示了如何关联于远程主机与用户，并要求在用户进入全局配置模式时发送 **auth** 身份认证级别 inform 通知。

```
Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Switch(config)# snmp-server group authgroup v3 auth
Switch(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5 mypassword
Switch(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Switch(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server inform retries 0
```

5.4.10 显示 SNMP 状态

可以使用 **show snmp** 特权模式命令显示 SNMP 输入和输出统计，包括非法的公共字符串条目、错误和被请求的变量。也可以使用表 5-23 中的其他特权命令来显示 SNMP 信息。

表 5-23 显示 SNMP 统计信息的命令

命令	功能
show snmp	显示 SNMP 统计
show snmp engineID	显示本地 SNMP 引擎和在设备中配置的所有远程引擎信息
show snmp group	显示网络中的每个 SNMP 组信息
show snmp pending	显示在排队等待的 SNMP 请求信息
show snmp sessions	显示当前会话的 SNMP 信息
show snmp user	显示在 SNMP 用户表中的每个 SNMP 用户信息

【注意】不支持 **snmp-server enable informs** 命令来启用 SNMP。要启用 SNMP 通知发送，可组合使用 **snmp-server enable traps** 命令和 **snmp-server host *host-addr* informs** 命令。

5.5 配置 IP 单播路由

本节介绍如何在 Cisco Catalyst 交换机上配置 IPv4 单播路由。本部分本来涉及许多比较难以理解的动态路由协议，如 RIP、OSPF、BGP、EIGRP 等，但对于交换机来说，路由功能相对较弱，所以在此也不进行太多路由协议和复杂功能的配置。有关路由协议的更详细介绍参见笔者的另一本书《路由器配置完全手册》。

5.5.1　理解 IP 路由

在一些网络环境中，VLAN 是与具体的网络或者子网相关联的。在一个 IP 网络中，每个子网是被映射到一个具体的 VLAN。配置配置有静默于控制广播域的大小和保持本地网络通信。无论如何，在没有三层设备（包括路由器和三层交换机）来在 VLAN 间路由通信的前提下，在不同 VLAN 中的网络设备是不能与其他 VLAN 中的设备相互通信的，这就是通常所说的 VLAN 间路由。可以配置一个或多个路由器来路由通信在目的 VLAN。

图 5-10 所示为一个基本的路由拓扑结构。交换机 A 在 VLAN10 中，交换机 B 在 VLAN20 中，两个 VLAN 通过 ISL 协议中继。路由器通过两个接口连接这两个 VLAN。

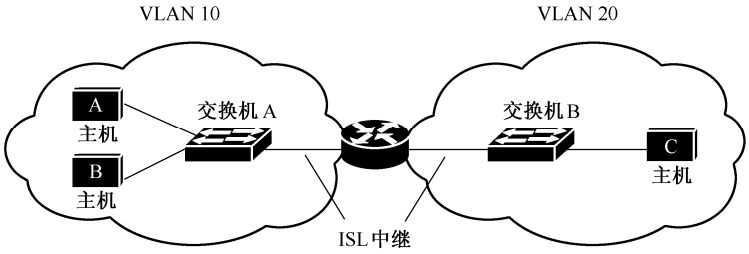

图 5-10　路由拓扑结构示例

当位于 VLAN10 中的主机 A 需要与 VLAN10 中的主机 B 进行通信时，它发送一个数据包到主机 B，此时交换机 A 直接转发数据包到主机 B，而不要发送到路由器，因为它们位于同一 VLAN 中。而当主机 A 发送一个数据包到位于 VLAN20 中的主机 C 时，交换机 A 转发数据包到路由器，在 VLAN 10 接口上接收到交换机 A 发送来的数据包。路由器检查路由表，找到正确的输出接口，并转发这个数据到 VLAN 20 接口上，然后再发送到交换机 B。交换机 B 在接收到数据包后再转发到主机 C。

路由器和三层交换机可以以下 3 种方式路由数据包：

（1）通过使用默认路由。

默认路由（也就是指默认网关）是指发送一个目标不明确的通信到路由器，然后再转发到一个默认的出口或者目的设备。有关默认网关的配置参见 5.5.3 节。

（2）通过使用预定的静态路由。

静态单播路由是从选定的端口转发数据包，通过单一路径流入或者流出网络。静态路由最大的优势就是安全、占用更小的网络带宽资源，但是它不能自动适应网络拓扑结构的变化，如某些链路失效会使得最终的通信不可达。随着网络规模的不断扩大，静态路由的应用越来越受限。

静态路由一般只在路由器上配置，在交换机上通常是使用默认路由和下面将要介绍的动态路由两种配置。

（3）通过使用路由协议来动态计算路由。

动态路由协议是由路由器（或者三层交换机）来动态计算转发具体通信时最佳的路由。有两种类型的动态路由协议：

- 路由器使用距离矢量协议（Distance-vector Protocol）来维护距离网络资源距离的路由表，并且周期性地传递这个路由表到邻居路由器上。距离矢量协议使用一个或者一系列的度量来计算最佳路由。这种动态路由协议的优点是比较容易配置和使用。
- 路由器使用链路状态协议（Link-state Protocol）依靠路由器间的链路状态通告（Link-state Advertisement，LSA）消息的交换来维护一个复杂的网络拓扑结构数据库。LSA 是由网络

中的事件触发的，如加速收敛速度和响应拓扑结构改变的时间。LSA 可以快速地响应拓扑结构改变，但是相比距离矢量路由协议来说，需要占用更多的网络带宽资源。

交换机支持的距离矢量协议是 RIP（Routing Information Protocol，路由信息协议），它是使用单一距离度量（消耗）来确定最佳路径的。另外交换机还支持 BGP（Border Gateway Protocol，边界网关协议）这个距离矢量路由协议，是一种添加了一个路径矢量的计算机制。交换机还支持 OSPF（Open Shortest Path First，开放最短路径优先）链路状态协议、EIGRP（Enhanced IGRP，增强型 IGRP），它是在 IGRP（Interior Gateway Routing Protocol，内部网关路由协议）的基础上添加了一些链路状态路由特征。

5.5.2 IP 路由接口和基本配置步骤

默认情况下，交换机上是禁止 IP 路由的，必须在需要路由时启用它。要启用路由的接口必须是以下 3 种三层接口类型之一：

- 路由端口：通过使用 **no switchport** 接口配置命令配置三层物理端口。
- 交换机虚拟接口（SVI）：通过使用 **interface vlan** *vlan_id* 全局配置命令创建的 VLAN 接口，默认为三层接口。
- 三层模式的以太网通道端口：通过使用“**interface port-channel** *port-channel-number*”全局配置命令创建的端口通道逻辑接口，是一组以太网接口绑定后形成的一个通道组。

【说明】交换机不支持在隧道接口上进行单播路由通信。三层交换机可以有分配给每个路由端口和 SVI 接口的 IP 地址。可以配置的路由端口和 SVI 接口数量在软件意义上是不受限制的，但受到像设备 CPU 等硬件性能配置的限制。

在所有配置了路由的三层接口上必须分配一个唯一的 IP 地址。

路由配置过程有以下几个主要的步骤：

（1）为了支持 VLAN 接口，在交换机或者交换机堆叠上创建和配置 VLAN，并且为二层接口分配 VLAN 成员。

（2）配置三层接口。

（3）在交换机上启用 IP 路由。

（4）为三层接口分配 IP 地址。

（5）在交换机上启用所选择的路由协议。

（6）配置路由协议参数（可选）。

5.5.3 配置 IP 地址

配置 IP 路由的一项任务就是为三层接口分配 IP 地址，以便启用接口，并允许使用 IP 地址与所连的主机进行通信。本节介绍如何配置不同的 IP 地址特性，具体如下（分配 IP 地址到接口是必须的，其他过程则是可选的）：

- 默认地址配置。
- 分配 IP 地址到网络接口。
- 配置地址的解析方法。
- 在禁用路由时的路由支持。
- 配置广播包处理。
- 监控和维护 IP 地址。

1．默认地址配置

表 5-24 所示为 Catalyst 交换机的默认地址配置。

表 5-24　Catalyst 交换机的默认地址配置

特征	默认设置
IP 地址	没有定义
ARP	在 ARP 缓存中没有参数项目。采用标准的以太网 ARP 协议封装。超时设置为 14400 秒（4 小时）
IP 广播地址	255.255.255.255（所有）
IP 无类别路由	启用
IP 默认网关	禁用
IP 直接广播	禁止，所有 IP 直接广播包都被丢弃
IP 域	域列表：没有定义域名称 域查询：启用 域命名：启用
IP 转发协议	如果定义了 helper 地址或者 UDP 泛洪广播，在默认端口上是启用转发的 任何本地广播：禁止 STP：禁止
IP helper 地址	禁止
IP host	禁止
IRDP	禁止，启用时默认配置如下： 广播 IRDP 通告 通告间的最大发送间隔：600 秒 通告间的最小发送间隔：0.75 倍最大间隔 优先权：0
IP 代理 ARP	启用
IP 路由	禁止
IP 零子网	禁用

2．为网络接口分配 IP 地址

一个 IP 地址标识了 IP 数据包可以被发送到的位置。有些 IP 地址是保留用于特殊用途的，不能用于主机、子网或者网络地址，如本地环路地址 127.1.0.0、0.0.0.0、广播地址等。

一个接口可以有一个主 IP 地址，掩码标识了 IP 地址中有多少位是用于标识网络的。当掩码用于网络中的一个子网时，此时的掩码就称为“子网掩码”。有关这方面的知识可以参见笔者编著的《网管员必读——网络基础》（第二版）。

从特权模式开始，按照表 5-25 所示的步骤来为一个三层接口分配 IP 地址和网络掩码。

表 5-25　为三层接口分配 IP 地址和网络掩码的步骤

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 IP 地址和网络掩码的三层接口，并进入接口配置模式
3	Switch(config-if)#**no switchport**	如果接口是物理接口，则把该接口从二层模式转换为三层模式
4	Switch(config-if)#**ip address** *ip-address subnet-mask*	为接口配置 IP 地址和子网掩码
5	Switch(config-if)#**no shutdown**	激活接口
6	Switch(config-if)#**end**	返回到特权模式
7	Switch#**show interfaces** [*interface-id*] Switch#**show ip interface** [*interface-id*] Switch#**show running-config interface** [*interface-id*]	校验以上设置
8	Switch#**copy running-config startup-config**	（可选）在当前运行的配置文件中保存以上设置

3．使用“子网 0”

在重新划分子网后的第一个子网的子网地址（亦即子网 ID，具体参见笔者编著的《网管员必读——网络基础》（第二版））是全为“0”的，这个子网一般是不建议使用的，因为这个子网的网

络地址与没有划分子网的原网络地址一样，这样一来就可能出现不能正确识别主机所在位置的现象。例如，如果 131.108.0.0 网络划分子网后的子网掩码为 255.255.255.0，这样第一个子网（也就是“子网 0”——Subnet Zero）的网络地址与没有划分子网的 131.108.0.0 网络的网络地址是一样的，都是 131.108.0.0。但是可以使用子网地址全为 1 的子网（本示例中为 131.108.255.0），即使我们不建议。

但在 Cisco 设备（包括交换机、路由器，甚至防火墙等）中，通过相应的配置，子网 0 同样是可以使用的，而且不会发生冲突，具体配置步骤如表 5-26 所示。本功能配置无须指定任何具体参数，所以可直接按表 5-27 中的配置方法进行配置。

表 5-26　使用“子网 0”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)#**ip subnet-zero**	为接口地址启用“子网 0”，并更新路由
3	Switch(config)#**end**	返回到特权模式
4	Switch#**show running-config**	校验以上设置
5	Switch)#**copy running-config startup-config**	（可选）在当前运行的配置文件中保存以上设置

使用 **no ip subnet-zero** 全局配置命令恢复默认设置，禁用子网 0。

4．无类别路由

默认情况下，在交换机配置了路由时是启用了无类别路由的。有了无类别路由，如果路由器接收到来自一个没有默认路由的网络的子网的数据包时，路由器将以最佳的路由转发该数据包。一个包含连续 C 类地址块空间的超网（Supernet）可用于模仿单一、大型的地址空间（如 B 类网络），设计用于减轻 B 类地址加速耗尽的压力。

如图 5-11 所示，启用了无类别路由。在主机（Host）发送一个数据包到 120.20.4.1 时，不会丢弃该数据包，路由器会以最佳的超网路由方式进行转发。相反，如果在路由器上没有启用无类别路由，当路由器接收到一个要去往一个没有默认路由网络的子网时，路由器会直接丢弃这个数据包，如图 5-12 所示。在这里要明白超网的计算方法。在本示例中，128.20.1.0、128.20.2.0 和 128.20.3.0 都是处于 128.20.0.0 这个超网之中，所以数据包会直接路由到网络 128.20.0.0 中的路由器上。具体的超网计算方法参见笔者编著的《网管员必读——超级网管经验谈》（第二版）一书。

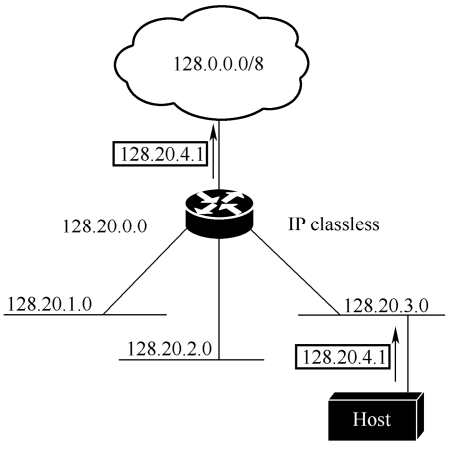

图 5-11　启用了无类别路由的示例

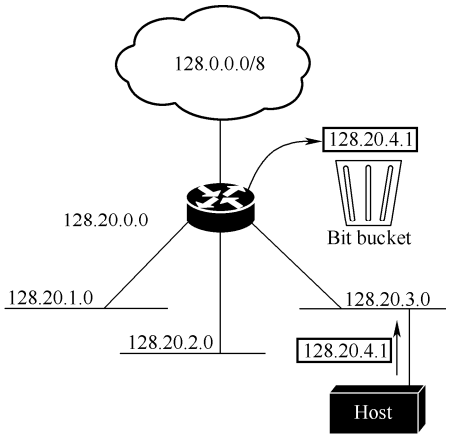

图 5-12　没有启用无类别路由的示例

在图 5-12 中，128.20.0.0 网络中的路由器同样是连接 128.20.1.0、128.20.2.0 和 128.20.3.0 这 3 个子网。但因为没有网络默认路由，也没有启用无类别路由，如果主机发送一个数据包到 120.20.4.1 子网中时，路由器会丢弃该数据包。

要阻止交换机以最佳超网路由方式转发数据包到不可识别的目的子网中，可以全局禁止无类别路由，方法如表 5-27 所示。本功能配置无须指定任何具体参数，所以可直接按表 5-27 中的配置方法进行配置。

表 5-27　禁用无类别路由的步骤

步骤	命令	用途说明
1	Switch#**configure terminal**	进入全局配置模式
2	Switch(config)#**no ip classless**	禁止无类别路由
3	Switch(config)#**end**	返回到特权模式
4	Switch#**show running-config**	校验以上设置
5	Switch#**copy running-config startup-config**	（可选）在当前运行的配置文件中保存以上设置

要恢复默认设置，使交换机可以以最佳超网路由方式转发数据包到没有网络默认路由的子网中，可以使用 **ip classless** 全局配置命令。

5.5.4　配置地址解析

可以通过使用地址解析来控制特定接口的 IP 处理方式。一个使用 IP 协议的设备可以有一个用来对设备在本地网段或者网络中进行唯一标识的 MAC 地址，同时还具有一个用来标识设备所在网络的网络地址。

MAC 地址是数据链路层地址，因为它包含在数据包头的数据链路层部分，并且只能由二层设备读取。在以太网中与其他设备的通信，软件必须学习到设备的 MAC 地址。这种从 IP 地址学习 MAC 地址的过程称为地址解析，而从 MAC 地址学习 IP 地址的过程称为反向地址解析。

交换机可以使用以下地址解析形式：

（1）ARP。ARP（Address Resolution Protocol，地址解析协议）用于关联 IP 地址和 MAC 地址。通过数据包中的 IP 地址，ARP 可以学习到对应的 MAC 地址，然后会在 ARP 缓存中存储这个 IP/MAC 地址关联表项，以便以后能快速地解析。当到达以太网内部后，IP 数据报就会以链路层的帧结构方式进行重新封装，然后以帧的方式发送到网络中的目的节点上。IP 数据报的封装和 ARP 请求，或者以太网以外的 IEEE 802 网络的应答是由 SNAP（Subnetwork Access Protocol，子网访问协议）说明的。

（2）Proxy ARP（代理 ARP）。Proxy ARP（代理 ARP）可以帮助没有路由表的主机学习其他网络上或者子网的主机的 MAC 地址。如果交换机（路由器）在与 ARP 请求发送者不一样的接口上接收到一个来自主机的 ARP 请求，并且路由器有通过其他接口到达主机的所有路由，它产生一个代理 ARP 包给它自己的本地数据链路地址。发送 APR 请求的主机发送它的数据包到路由器，然后再转发到目的节点。

（3）RARP（反向 ARP）。交换机也使用 RARP（Reverse Address Resolution Protocol，反向地址解析），它与 ARP 类似，只是 RARP 数据包请求的是 IP 地址，而不是本地 MAC 地址。使用 RARP 需要位于同一网段的一个 RARP 服务器作为路由器接口。可以使用 **ip rarp-server** *address* 接口配置命令来标识 RARP 服务器。

在配置地址解析时，可以完成以下任务：

- 定义静态 ARP 缓存。
- 设置 ARP 封装。
- 启用代理 ARP。

1．定义静态 ARP 缓存

ARP 和其他地址解析协议一样为 IP 地址和 MAC 地址提供动态映射。因为绝大多数主机支持动态平衡地址解析，通常不需要指定静态 ARP 缓存条目。如果必须定义 ARP 缓存条目，可以在 ARP 缓存中安装一个永久条目用于交换机从 IP 地址解析出 MAC 地址。也可以指定交换机响应 ARP 请求，好象它就是指定 IP 地址的拥有者一样（目前常被黑客利用进行地址欺骗）。如果不想要永久的 ARP 条目，可以为 ARP 条目指定一个有效期。

自特权模式开始，按照表 5-28 所示的步骤可以配置静态 IP 地址和 MAC 地址的映射。

表 5-28　配置 IP 地址与 MAC 地址映射的步骤

步骤	命令	用途说明
1	Switch#**configure terminal**	进入全局配置模式
2	Switch(config)#**arp** *ip-address hardware-address type*	在 ARP 缓存中全局关联一个 IP 地址和一个 MAC 地址，并且指定以下封装类型中的一个： ● arpa：以太网接口的 ARP 封装。 ● snap：令牌环和 FDDI 接口的子网访问协议（SNAP，Subnetwork Access Protocol）封装。 ● sap：HP 的 ARP 类型。
3	Switch(config)#**arp** *ip-address hardware-address type* [*alias*]	（可选）指定交换机响应 ARP 请求，好象它是指定的 IP 地址拥有者（ARP 欺骗就是利用了这一功能）
4	Switch(config)#**interface** *interface-id*	进入接口配置模式，指定要配置的接口
5	Switch(config-if)#**arp timeout** *seconds*	（可选）设置 ARP 缓存条目保存的时间长度，取值范围为 0～2147483 秒，默认为 14400 秒（4 小时）
6	Switch(config-if)#**end**	返回到特权模式
7	Switch#**show interfaces** [*interface-id*]	校验 ARP 类型和所有或者特定接口上配置的 ARP 条目的保存时间
8	Switch#**show arp** 或者 Switch#**show ip arp**	校验 ARP 缓存内容
9	Switch#**copy running-config startup-config**	（可选）在当前运行的配置文件中保存以上设置

要从 ARP 缓存中删除 ARP 条目，可以使用 **no arp** *ip-address hardware-address type* 全局配置命令，要删除 ARP 缓存中的所有非静态条目，可以使用 **clear arp-cache** 特权模式命令。

2．设置 ARP 封装

默认情况下，在 IP 接口上是启用以太网 ARP 封装的。如果需要，也可以设封装方式为 SNAP 方法。自特权模式开始，按照表 5-29 所示的步骤来设置指定的 ARP 封装类型。

表 5-29　设置 ARP 封装类型的步骤

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*	指定要配置的三层接口，并进入接口配置模式
3	Switch(config-if)#**arp** {**arpa** | **snap**}	指定 ARP 封装方法： ● arp：ARP 协议封装 ● snap：SNAP 协议封装
4	Switch(config-if)#**end**	返回到特权模式
5	Switch#**show interfaces** [*interface-id*]	校验所有/特定接口上的 ARP 封装配置
6	Switch#**copy running-config startup-config**	（可选）在当前运行的配置文件中保存以上设置

要禁止封装类型，可以使用 **no arp arpa** 或者 **no arp snap** 接口配置命令。

3．启用代理 ARP

默认情况下，交换机使用 ARP 来帮助主机学习其他网络或者子网中主机的 MAC 地址。自特权模式开始，按照表 5-30 所示的步骤来启用代理 ARP。

表 5-30　启用代理 ARP 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*	指定要配置的三层接口，并进入接口配置模式
3	Switch(config-if)#**ip proxy-arp**	在接口上启用代理 ARP
4	Switch(config-if)#**end**	返回到特权模式
5	Switch#**show ip interface** [*interface-id*]	校验接口上的代理 ARP 配置
6	Switch#**copy running-config startup-config**	（可选）在当前运行的配置文件中保存以上设置

要禁用代理 ARP，可以使用 **no ip proxy-arp** 接口配置命令。

5.5.5　在禁用 IP 路由时的路由辅助

在禁止 IP 路由的情况下，以下机制可以允许交换机学习到达其他网络的路由。

- 代理 ARP
- 默认网关
- ICMP 路由器发现协议

1．代理 ARP（Proxy ARP）

代理 ARP 是最常用的学习其他路由的方法，使得以太网主机可以在没有路由信息的情况下与其他网络或者子网的主机进行通信。在代理 ARP 协议的帮助下，主机假设所有主机位于同一个本地以太网上，它可以使用 ARP 协议来学习它们的 MAC 地址。如果交换机接收到一个访问本地网络中主机的请求，而 ARP 请求是从不同网络中的远程主机发出的，此时交换机会评价是否有从该主机到达远程网络主机最佳的路由。如果有，本地网络主机发送一个带有自己 MAC 地址的 ARP 应答，通过交换机转发到远程主机。代理 ARP 会协商通信双方网络，就像它们在同一个网络中一样为每个 IP 地址执行 ARP 请求。

在交换机上代理 ARP 默认是启用的，如果在禁止后要重新启动，请按照上节第 3 小点介绍的方法进行配置。但要注意的是，要使用代理 ARP，必须网络中的其他路由器也必须支持它。

2．默认网关

另一种定位路由的方法是定义默认路由器或者默认网关。所有发送到非本地的包先发送到路由器，然后由路由器要么进行适当路由，要么返回一个 ICMP 重定向消息，指出主机应当使用哪个本地路由器。交换机会缓存这条重定向消息，并尽力转发每个包。这种方法的局限性是在默认路由器关机或者无效时没有办法检测到。

自特权模式开始，按照表 5-31 所示的步骤为在没有 IP 路由的情况下定义默认网关或者默认路由器。

表 5-31　默认网关的配置步骤

步骤	命令	用途说明
1	Switch#**configure terminal**	进入全局配置模式
2	Switch(config)#**ip default-gateway** *ip-address*	设置默认网关或者默认路由器
3	Switch(config)#**end**	返回到特权模式
4	Switch#**show ip redirects**	显示默认网关 IP 地址
5	Switch#**copy running-config startup-config**	（可选）保存配置在启动配置文件中

可以使用 **no ip default-gateway** 全局配置命令禁止默认网关功能。

3．IRDP（ICMP Router Discovery Protocol，ICMP 路由器发现协议）

IRDP 是一个使用 ICMP（Internet Control Message Protocol，互联网控制消息协议）消息对来选择路由器的发现方法，主要用于多播链路中。IRDP 可以免除手动配置路由器地址的麻烦，而且与任何指定的路由协议无关。

主要在它们可以发送 IP 数据报到它们的子网前必须发现路由器 IP 地址。通常这是在启动时通过读取配置文件中的一个或者多个路由器地址来实现的。在多播链路中，有些主机也可以通过侦听路由协议通信来发现路由器地址。以上这两种方法存在严重的缺陷：配置文件都必须手工维护，管理负担较重，而且不能动态地跟踪路由器可能的改变。

IRDP 使用 ICMP 路由器广告和路由器触发消息来允许主机发现子网上运行路由器的地址。每个路由器周期性地从它的多播接口上广播一个个路由器广告，宣告该路由器的接口 IP 地址。主机侦听这种广告，以发现邻居路由器的地址。当主机在一个多播链路上启动时，它可能发送一个多播路由器触发消息，以请求运行了 IRDP 协议的路由器立即发送路由器地址广告，而不用等待下次发送广告的时间到来。如果主机仍没有接收到路由器地址广告，主机可能会少数次发送触发消息，当然最后仍没有收到的话，也不会继续发送了。任何后来启动的路由器，或者因为路由器地址广告包丢失，或者临时性的链路失效没有被发现的路由器，最终会通过接收周期性的路由器地址广告而被发现。

ICMP 路由器发现消息不是路由协议。它可以使主机发现已有的邻居路由器，但是不能确定哪个路由器路径是到达指定目标的最佳路径。如果一个主机为一个特定的目标选择了一个不是很好的下一跳路由器，则它应当会从路由器上接收到一个 ICMP 重定向消息，指出一条更好的路径。

每个被主机发现的设备都会被当作默认路由器的候选设备，当发现了一个较高优先级的路由器，或者在当前默认路由器宣传关闭，或者与该路由器的 TCP 连接因过多的重传而超时时，就会选择一个新的最高优先级路由器。这对于接口上的 IRDP 路由来说唯一的任务是在接口上启用 IRDP 进程。在启用 IRDP 时，将会应用默认参数。当然，也可以随意改变这些参数，方法如表 5-32 所示。

表 5-32　启用和重新配置 IRDP 协议的步骤

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*	指定要启用 IRDP 协议的三层接口，并进入接口配置模式
3	Switch(config-if)#**ip irdp**	在上述接口上启用 IRDP
4	Switch(config-if)#**ip irdp multicast**	（可选）在多播地址（224.0.0.1）上发送 IRDP 广告，而不用 IP 广播
5	Switch(config-if)#**ip irdp holdtime** *seconds*	（可选）设置 IRDP 广告的有效期。默认是 3 倍于下一步将要配置的 maxadvertinterval 参数值，必须大于 maxadvertinterval 参数值，而小于 9000 秒。如果改变了 maxadvertinterval 参数值，则这个值也将改变
6	Switch(config-if)#**ip irdp maxadvertinterval** *seconds*	（可选）设置 IRDP 最大的广告发送间隔。默认值为 600 秒
7	Switch(config-if)#**ip irdp minadvertinterval** *seconds*	（可选）设置 IRDP 最小的广告发送间隔。默认值是 0.75 倍于上一步配置的 maxadvertinterval 参数值。如果改变了 maxadvertinterval 参数值，则这个值也将改变为新的默认值（0.75 倍于 maxadvertinterval 参数值）
8	Switch(config-if)#**ip irdp preference** *number*	（可选）设置接口的 IRDP 优先级别。允许的值在-2^{31}～2^{31}之间，默认值为 0，数值越大，级别越高
9	Switch(config-if)#**ip irdp address** *address* [*number*]	（可选）指定一个 IRDP 地址用于优先代理广告
10	Switch(config-if)#**end**	返回到特权模式
11	Switch#**show ip irdp**	校验 IDRP 设置
12	Switch#**copy running-config startup-config**	（可选）在启动配置文件中保存设置

如果改变了 **maxadvertinterval** 参数值，则 **holdtime** 和 **minadvertinterval** 将同时发生改变，所以它是非常重要的。使用 **no ip irdp** 接口配置命令可以禁止 IRDP 路由。

5.5.6　配置广播包处理

在配置了 IP 地址后，可以启用路由，配置一个或者多个路由协议，或者可以配置交换机响应网络广播的方法。广播是指数据包的目的地址是一个物理网络中的所有主机。交换机支持两种类型的广播：

- 定向广播包是发送到指定网络或者一系列网络中的主机上。直接广播地址包括网络或者子网字段。
- 泛广播包是发送到任意网络中。

路由器通过限制它们到本地电缆的范围来提供一些阻止广播风暴的保护。因为网桥属于二层设备，转发所有广播到所有网络网段，这样就可能产生广播风暴。解决广播风暴的最好方法是在一个网络中使用单一广播地址方案。不过，目前在多数 IP 设施中，可以设置使用一个广播地址。许多设施，包括交换机，支持多个转发广播消息的地址分配方案。

1．启用定向广播（Directed Broadcast）到物理广播（Physical Broadcast）转换

默认情况下，定向 IP 广播包是被丢弃不被转发的。丢弃定向 IP 广播可以使路由器减轻遭受拒绝服务攻击的风险。

可以在有广播包的接口上启用定向 IP 广播（IP-Directed Broadcast）转换为物理广播（Physical Broadcast，也就是基于 MAC 地址的二层广播）的转发功能，仅需要使用 **ip forward-protocol** 全局配置命令即可。

可以指定一个访问列表来控制哪些广播可以被转发。在指定了访问列表后，仅访问列表中的 IP 包允许从定向广播转换成物理广播。

从特权模式开始，按照表 5-33 所示的步骤启用接口上的定向 IP 广播转发。

表 5-33　在接口上启用定向广播的步骤

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	Switch(config-if)#**ip directed-broadcast** [*access-list-number*]	在接口上启用直接广播到物理广播的转换。可以包括一个访问列表来控制哪些广播包可以被转发。在配置了访问列表后，仅在列表中的 IP 包可以被转换。 **ip directed-broadcast** 接口配置命令可以在 VPN 路由/转发（VPN routing/forwarding，VRF）接口上配置。直接广播通信仅在 VRF 中可以被路由
4	Switch(config-if)#**exit**	返回到全局配置模式
5	Switch(config)#**ip forward-protocol** {**udp** [*port*] | **nd** | **sdns**}	指定路由器在转发广播包时可用的协议和端口。 **udp**：转发 UDP 数据报 *port*：指定控制转发哪个 UDP 服务的指定端口 **nd**：转发 ND 数据报 **sdns**：转发 SDNS 数据报
6	Switch(config)#**end**	返回到特权模式
7	Switch)#**show ip interface** [*interface-id*] 或者 Switch#**show running-config**	校验接口上的以上配置
8	Switch#**copy running-config startup-config**	（可选）在当前运行的配置文件中保存以上设置

使用 **no ip directed-broadcast** 接口配置命令来禁用定向广播到物理广播的转换，使用 **no ip forward-protocol** 全局配置命令来删除一个协议或者端口。

2．转发 UDP 广播包和协议

UDP 与 TCP 一样是一个 IP 主机到主机层协议。UDP 在两个终端系统之间提供一个低开销、

不面向连接的会话，但不对接收到的数据报提供确认。网络主机偶尔使用 UDP 广播来发现地址、配置和名称信息。如果在不包括服务器的网络段中有这样一台主机，UDP 广播通常是不被转发的。可以通过配置路由器的一个接口来转发某种类型的广播包到一个帮助地址（Helper Address）。可以在一个接口上使用更多的帮助地址。

【说明】Helper-address 用来转发 UDP 广播，和 IP Forward-protocol（IP 转发协议）组合使用，可以控制哪些 UDP 广播包可以被转发。Cisco 路由器允许用 no ip forward-protocol udp 命令来禁止对无意义的 UDP 数据报的转发。

可以指定一个 UDP 目的端口来控制哪个 UDP 服务补转发，可以指定多个 UDP 服务。可以指定网络磁盘（Network Disk，ND）协议和网络安全协议 SDNS。ND 用于早期的 SUN 无盘工作站中。默认情况下，如果基接口上定义了 Helper Address（帮助地址），UDP 和 ND 转发是启用的。如果在配置 UDP 广播转发时没有指定任何 UDP 端口，则要配置路由器作为 BOOTP 转发代理。BOOTP 包承载了 DHCP 信息。

从特权模式开始，按照表 5-34 所示的步骤来在接口上启用 UDP 广播包转发，并指定广播包转发的目的帮助地址。

表 5-34　在接口上启用 UDP 广播包转发并指定目的帮助地址的步骤

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*	指定要配置的三层接口，并进入接口配置模式
3	Switch(config-if)#**ip helper-address** *address*	启用 UDP 广播包（包括 BOOTP 包）转发并指定目的帮助地址
4	Switch(config-if)#**exit**	返回到全局配置模式
5	Switch(config)#**ip forward-protocol** {**udp** [*port*] | **nd** | **sdns**}	指定可以转发的广播包协议
6	Switch(config)#**end**	返回到特权模式
7	Switch#**show ip interface** [*interface-id*] 或者 Switch)#**show running-config**	校验接口上的以上设置
8	Switch#**copy running-config startup-config**	（可选）在当前运行的配置文件中保存以上设置

使用 **no ip helper-address** 接口配置命令来禁止广播包转发到指定的帮助地址，使用 **no ip forward-protocol** 全局配置命令来删除可以转发的广播包协议。

3．建立广播地址

大多数常规的 IP 广播地址是包含所有主机的 255.255.255.255 地址，但交换机可以配置产生任何格式的 IP 广播地址。

从特权模式开始，按照表 5-35 所示的步骤来为接口创建新的广播地址。

表 5-35　为接口创建新的广播地址的步骤

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	Switch(config-if)#**ip broadcast-address** *ip-address*	键入一个不同于默认的 255.255.255.255 的广播地址，如 128.1.255.255
4	Switch(config-if)#**end**	返回到特权模式
5	Switch#**show ip interface** [*interface-id*]	校验接口上的以上设置
6	Switch#**copy running-config startup-config**	（可选）在当前运行的配置文件中保存以上设置

要恢复到默认的广播地址（255.255.255.255），可以使用 **no ip broadcast-address** 接口配置命令。

5.5.7　启用 IP 单播路由

默认情况下，交换机是二层交换模式的，并禁用 IP 路由。要使用交换机的三层功能，就必须

启用 IP 路由。

从特权模式开始，按照表 5-36 所示的步骤可以启用 IP 路由。

表 5-36　启用 IP 路由的步骤

步骤	命令	用途说明
1	Switch#**configure terminal**	进入全局配置模式
2	Switch(config)#**ip routing**	启用 IP 路由
3	Switch(config)#**router** *ip_routing_protocol*	指定一个 IP 路由协议。但要注意，使用 IP 基础映象（IP Base Image）文件的交换机仅支持 RIP 作为路由协议
4	Switch(config)#**end**	返回到特权模式
5	Switch#**show running-config**	校验以上设置
6	Switch#**copy running-config startup-config**	（可选）在当前运行的配置文件中保存以上设置

可以使用 **no ip routing** 全局配置命令来禁用 IP 路由。

以下是一个显示如何启用使用 RIP 路由协议的 IP 路由的示例。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# end
```

可以通过像 RIP、OSPF、EIGRP、BGP 等的动态路由协议来配置 IP 路由。因为这些路由协议在笔者编著的《路由器配置与管理完全手册》中有全面的配置方法介绍，而且交换机中的配置方法与路由器的这些路由协议配置很类似，况且在交换机上使用动态路由协议并不是很多，所以从下节开始仅介绍相对来说较为简单的 RIP 和 OSPF 协议的配置方法。

5.6　配置 RIP

RIP（Routing Information Protocol，路由信息协议）是一个 IGP（Interior Gateway Protocol，内部网关协议），主要用于同种网络间的路由。它是一种使用 UDP 数据报以广播方式交换路由信息的距离矢量动态路由协议。

【说明】RIP 仅支持 IP 基础映象（IP Base Image）文件的交换机系统，其他路由协议需要交换机堆叠主运行 IP 服务映象（IP Service Image）。

有关像 RIP、OSPF、IS-IS 等的路由协议将在后面介绍 H3C 交换机路由配置时有详细介绍，在此不再赘述了，详情参见第 21 章。

使用 RIP 路由协议，交换机会每隔 30 秒发送一次路由信息更新。如果一个路由器在 180 秒内没有接收到从其他路由器发送来的路由信息更新，则将标记相应路由器不可用。如果直到 240 秒仍不能接收到更新，路由器将从路由表中删除那些不能更新的路由器条目。

RIP 协议使用跃点（hop）数来计算不同路由值。hop 是指在一条路由所经过的路由器数。直接连接网络则称 hop 数为 0，达到 16 则表示网络不可达。所以，RIP 路由中的 hop 取值范围是 0～15，这也决定了它仅可以应用于小型网络。

如果路由器有一个默认的网络路径，RIP 通告一个链接路由器到 0.0.0.0 这样的虚构网络的路由。0.0.0.0 网络并不存在，它只是用于 RIP 来执行默认路由功能。在 RIP 学习到一个默认路由，或者路由器有一个更短路径的网关，则交换机会通告这个默认路由，并且 RIP 会以这个默认路径度量进行配置。RIP 发送路由信息更新到指定网络的接口上。如果接口所在网络没有指定，则不通告任何 RIP 更新。

5.6.1 配置基本 RIP 参数

要配置 RIP，需要为网络启用 RIP 路由，通常也需要配置其他参数。从特权模式开始，按照表 5-37 所示的步骤来启用 RIP 路由，并配置 RIP 参数。

表 5-37 配置基本 RIP 参数的步骤

步骤	命令	用途说明
1	Router# **configure terminal**	进入全局配置模式
2	Router(config)#**ip routing**	启用 IP 路由（仅在当前 IP 路由禁止时）
3	Router(config-router)# **router rip**	启用 RIP 路由，并进入路由器配置模式
4	Router(config-router)#**network** *network number*	指定与 RIP 路由进程关联的网络（也就是要使用 RIP 所配置的路由的网络）。可以使用多个 **network** 命令。RIP 路由更新仅在指定的这些网络中发送和接收。注意，必须为生效的 RIP 命令配置至少一个网络地址
5	Router(config-router)#**neighbor** *ip-address*	（可选）定义一个用于交换路由信息的邻居路由器，以允许 RIP 路由更新到达非广播网络
6	Router(config-router)#**offset list** [*access-list number* | *name*] {**in** | **out**} *offset* [*type number*]	（可选）应用一套路由度量偏移列表用于增加通过 RIP 学习到的流入和流出路由度量。可以用一个访问列表或者接口来限制偏移列表
7	Router(config-router)#**timers basic** *update invalid holddown flush*	（可选）调整路由协议计时器。取值范围为 0～4294967295 秒。 ● *update*：发送路由更新的时间，默认值为 30 秒。 ● *invalid*：路由器被公告无效的计时器，默认为 180 秒。 ● *holddown*：路由从路由表中删除前的时间，默认为 180 秒。 ● *flush*：路由更新延迟的时间，默认为 240 秒。
8	Router(config-router)#**version** {**1** | **2**}	配置交换机接收和发送的 RIP 包版本。默认情况下，Catalyst 3500、Catalyst 3750 系列交换机可以接收版本 1 和版本 2 RIP 包，但仅能发送版本 1 RIP 包。可以使用 **ip rip** {**send** | **receive**} **version 1** | **2** | **1 2** 命令来控制接口可以发送和接收的版本
9	Router(config-router)#**no auto summary**	（可选）禁止自动汇总。默认情况下，交换机在类网络边界处汇总前缀。禁止汇总广告子网和主机路由信息到类网络边界
10	Router(config-router)#**no validate-update-source**	（可选）禁止流入 RIP 路由更新的 IP 地址资源的验证。默认情况下，交换机验证这些资源的有效性，如果资源无效，则放弃资源的更新。但通常情况下是不建议禁止的。但如果有一个离线的路由器，而你又想接收到它的更新，则可以使用这个命令
11	Router(config-router)#**output-delay** *delay*	（可选）为 RIP 更新包发送添加包内延时。默认情况下，在一个多包 RIP 更新的包之间是不会添加包延时的。如果是通过低速率设备发送包，则可以添加一个包内延时，取值范围为 8～150 毫秒
12	Router(config-router)#**end**	返回到特权模式
13	Router#**show ip protocols**	显示当前活动路由协议的参数配置和状态
14	Router#**copy running-config startup-config**	在当前运行的配置文件中保存以上设置

可以使用 **no router rip** 全局配置命令关闭 RIP 路由进程。

5.6.2 配置 RIP 身份认证

RIP 版本 1 不支持身份认证。但如果发送和接收的是 RIP 版本 2 包，则可以在接口上启用 RIP 身份认证。RIP 密钥链（Key Chain）指定了在接口中可以使用的一套密钥。如果没有配置密钥链，则不能执行身份认证。

交换机在接口上支持两种 RIP 身份认证模式：明文（Plain Text）和 MD5（消息摘要 5），默认为明文认证模式。从特权模式开始，按照表 5-38 所示的步骤来为接口配置 RIP 身份认证。

要恢复纯文本身份认证（也就是明文身份认证），可以使用 **no ip rip authentication mode** 接口配置命令；要阻止身份认证，则可以使用 **no ip rip authentication key-chain** 接口配置命令。

表 5-38　配置接口 RIP 身份验证的步骤

步骤	命令	用途说明
1	Route#**configure terminal**	进入全局配置模式
2	Router(config)#**interface** *interface-id*	指定要配置的接口，并进入接口配置模式
3	Router(config-if)#**ip rip authentication key-chain** *name-of-chain*	启用 RIP 身份认证，并指定密钥链名称
4	Router(config-if)#**ip rip authentication mode** [**text** | **md5**}	配置接口使用明文（默认模式）或者 MD5 摘要身份认证
5	Router(config-if)#**end**	返回到特权模式
6	Router#**show running-config interface** [*interface-id*]	校验以上设置
7	Router#**copy running-config startup-config**	（可选）在当前运行的配置文件中保存以上设置

5.6.3　RIP 路由汇总配置

RIP v2 中的路由汇总功能可以提高大型网络的可用性和运行效率。汇总 IP 地址意味着在 RIP 路由表中无须为子路由器配置路由条目，减少路由表大小，以使得路由效率更高。路由汇总是通过多个连续子网前缀的比较找出相同位数得出子网掩码的。路由汇总与可变长子网掩码（VLSM）相关联。

在此处介绍的 RIP，以及后面将要介绍的 OSPF 等动态路由协议中都会有一种称为“路由汇总”的功能。这里关键是要理解“汇总”这两个字，它是指把多条小范围的路由汇总成一条大范围的路由。如多个子网路由就可以汇总成一条对应的有类别网络路由。这其实就是与 VLSM 中的“超网”（有关“超网”的计算可参见笔者编著的《网管员必读——超级网管经验谈》（第二版）一书）。很显然这样做的目的就是为了减少路由表的体积，使查询效率更高。

1．路由汇总的优势和使用条件

广告一条汇总 IP 地址功能比广告多个 IP 路由更有效的原因如下：

- 在 RIP 数据库中的汇总路由是优先处理的。
- 所有包含在汇总路由中的子路由都将在查询数据库时被跳过，减少查询时间。

Cisco 路由器可以采用两种方法汇总路由：

- 自动汇总：通过汇总子网前缀到有类别网络边界实现。也可以这么理解，自动汇总总是包括了最大的网络范围，而可能不是最适宜的路由。如 10.1.1.0/24、10.1.2.0/24、10.1.3.0/24 这 3 个子路由最终的自动汇总结果是 10.0.0.0/8 这个 A 类网络地址，而这 3 个子路由的实际最佳汇总路由应该是 10.1.0.0/16。因为这个地址同样包含了以上 3 个子网，同时这样的路由也可使选择的主机范围更加精确。

【说明】无须为启用自动汇总进行任何配置，因为这是默认设置。但是如果要禁止自动汇总，则可以使用 **no auto-summary** 路由器配置命令。

- 手工汇总：在指定接口上广告一个汇总的本地 IP 地址池，以便地址池可以被拨号客户端使用。

在指定接口上使用 **ip summary-address** 路由器配置命令汇总地址时，自动汇总地址总是汇总到有类别网络地址的边界（也就是这个汇总的地址都是像以 A、B、C 类划分的网络地址，而不可能是一个子网地址）。如果启用了自动汇总，则路由器上的接口就默认具有这种功能，而不管拨入的客户端是否使用了 **ip summary-address rip** 命令。

例如，如果在网络访问服务器上配置了一个从 10.1.1.1 到 10.1.1.254 的本地地址池，则可以在为拨号客户端提供地址的网络访问服务器端口配置 **ip summary-address rip 10.1.1.0 255.255.255.0**

命令，以使路由器广告 10.1.1.0/24 路由到拨号客户端。因为广告了一个汇总路由，像前缀“/32”这样的非有类别网络边界的主机路由广告将被抑制，路由器也不会广告这样的路由到网络访问服务器接口。

自动汇总将覆盖指定接口上所配置的汇总地址，除了以下两种情况外：

- 配置的接口汇总地址和接口配置的 IP 地址同属于一个主网络（也就是一个有类别网络，而不是划分后的子网）。
- 在接口上没有启用 Split horizon（水平分割）算法。

以下示例显示了在 RIP 中，**ip summary-address rip** 路由器配置命令是如何与自动汇总路由一起工作的。在示例中，主网络是 10.0.0.0，A 类网络，允许的空间是 0.*x*.*x*.*x*（其中 *x* 用于定义网络主机的位置）。主网络汇总定义了由有类别网络（A、B、C 类）地址默认的地址前缀（A 类为“/8”，B 类为“/16”，C 类为“/24”），实际表示形式中是不用带任何地址前缀的。汇总地址 10.2.0.0 覆盖 10.0.0.0 的自动汇总地址，这样，10.2.0.0 路由地址将在接口 E1 上广告，而不广告 10.0.0.0 路由地址，因为没有启用 Split horizon。

```
Router(config)# interface Ethernet1
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0   !--设置汇总路由地址为 10.2.0.0，子网掩码 255.255.0.0。显然不是
!--一个标准的有类别网络地址，而是一个重新划分了子网的网络地址
Router(config-if)# no ip split-horizon     !--不启用 split-horizon 路由算法
Router(config-if)# exit
Router(config)# router rip
Router(config)# network 10.0.0.0   !--指定要应用 RIP 路由的网络——10.0.0.0
```

当 RIP 确定在 RIP 数据库中是需要汇总路由时，一个汇总条目就会在 RIP 路由数据库中创建。只要有为汇总地址的子路由，在路由数据库中的地址就会保持。在最后一个子路由删除后，则汇总路由也将从路由数据库中删除。这种处理数据库条目的方法减少了数据库中的条目数量，因为每个子路由不会在路由条目中列出，在不再有任何子路由时，所有路由也会自己删除。

RIP v2 路由汇总需要广告所有条目中最佳路由的最低度量或者所有当前子路由器的最低度量。汇总路由的最佳度量是在路由初始化或者在指定路由广告，而不是在所有路由广告的过程中修改了度量时计算出来的。

2．在接口上配置路由汇总

ip summary-address rip 路由器配置命令会引起路由器汇总一系列通过 RIP v2 或者重新分配到 RIP v2 的给定路由（主机路由特别适合于进行路由汇总）。可以使用表 5-39 所示的步骤自全局配置模式开始进行 IP 汇总地址配置。

表 5-39　在接口上配置路由汇总的步骤

步骤	命令	用途说明
1	Router(config)# **interface** ***type number***	进入接口配置模式
2	Router(config-if)# **ip summary-address rip** *ip-address network-mask*	指定用于标识要用于汇总的路由的 IP 地址和网络掩码

3．校验 IP 路由汇总

可以使用 **show ip protocols** 特权模式命令校验接口上哪条路由被汇总了。以下示例显示了隐含的汇总和 Ethernet2 接口中关联的接口汇总和网络掩码（没有启用自动汇总，注意输出信息中的粗体字部分）。

```
Router# show ip protocols
 Routing Protocol is "rip"
    Sending updates every 30 seconds, next due in 8 seconds
    Invalid after 180 seconds, hold down 180, flushed after 240
    Outgoing update filter list for all interfaces is
```

```
Incoming update filter list for all interfaces is
Redistributing: rip
Default version control: send version 2, receive version 2
  Interface          Send  Recv  Triggered RIP  Key-chain
  Ethernet2          2     2
  Ethernet3          2     2
  Ethernet4          2     2
  Ethernet5          2     2
Automatic network summarization is not in effect
Address Summarization:
  10.11.0.0/16 for Ethernet2
```

可以检查 RIP 数据库中的汇总地址条目。仅当相关的子路由被汇总时才会在数据库中显示汇总地址条目。当与汇总地址关联的子路由无效时，则这个汇总地址也会从路由表中被删除。以下示例显示了一个包含 3 个子路由的 10.11.0.0/16 路由的汇总地址。

```
router# show ip rip database

10.0.0.0/8      auto-summary
10.11.11.0/24    directly connected, Ethernet2
10.1.0.0/8      auto-summary    !--自动汇总地址
10.11.0.0/16    int-summary     !--最终汇总地址
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
10.11.10.0/24    directly connected, Ethernet3
10.11.11.0/24    directly connected, Ethernet4
10.11.12.0/24    directly connected, Ethernet5
```

4．禁止自动路由汇总

RIP v2 默认是支持自动路由汇总的。它是汇总地址前缀到有类别网络边界，也就是汇总成最适合的对应有类别网络地址。如果有没有连接的子网，禁止自动路由汇总广告对应子网。当路由汇总禁止时，RIP 会发送子网和主机信息到整个有类别网络边界。要禁止自动汇总，可以使用 **no auto-summary** 路由器配置模式命令。

5.6.4　RIP 的其他配置

除了前面的一些主要 RIP 功能配置外，还可以配置一些其他相对较次要的功能，如本节将要介绍的禁止源 IP 地址确定、禁止或者启用 Split Horizon，以及 RIP 包间延时。

1．禁止源 IP 地址确认

默认情况下，RIP 系统会确认流入 RIP 路由更新中的源 IP 地址。只有有效的路由地址才接收更新，如果源地址无效，则 RIP 软件会放弃这个路由更新。如果当前有一个路由器不能正常工作，而又想接收它的路由更新，则可以在交换机上配置 RIP 禁止源 IP 地址确认功能。但这并不是建议的做法。

要禁止源 IP 地址确认功能，可以使用 **no validate-update-source** 路由器配置模式命令进行配置。

2．启用或禁止 Split Horizon

通常情况下，连接到广播类型的 IP 网络中的路由器会使用距离矢量（Distance-Vector）路由协议完成 Split Horizon（水平分割）机制，以减少所需的路由跳数。Split Horizon 会阻止被路由器广告的路由信息流出任何信息发出的路由接口。这种功能通常用于优化多个路由器间的通信，特别是存在链路失效时。但是，对于非广播类型网络（如 FR（Frame Relay，帧中继）和 SMDS（Switched Multimegabit Digital System，交换式多兆位数据系统））中则比较少用 Split Horizon 功能，所以可以禁止 RIP 的这种 Split Horizon 功能。

要在接口上启用 Split Horizon 功能，可以使用 **ip split-horizon** 命令接口配置模式命令；要在接口上禁止 Split Horizon 功能，可以使用 **no ip split-horizon** 接口配置模式命令。

3．配置包间延时

默认情况下，在发送多个 RIP 更新包时会在发送包间添加一个延时。如果是用一个高性能路由器向低性能路由器发送更新包，则可能需要添加这样一个延时到 RIP 更新包中。延时的取值范围为 8～50 毫秒。配置包发送过程中的包间延时可以使用 **output-delay** *milliseconds* 路由器配置模式命令。

5.7 配置 OSPF

本节介绍如何在思科交换机上配置 OSPF（Open Shortest Path First，开放最短路径优先）路由协议。OSPF 区分不同的网络为：广播、非广播、点对点网络类型。思科交换机支持广播网络（如以太网、令牌环和 FDDI 网络）和点对点（配置为点对点链路的以太网接口）网络。

5.7.1 OSPF 概述

OSPF 路由协议是一种典型的链路状态（Link-state）路由协议，一般用于同一个路由域内。在这里，路由域是指一个自治系统（Autonomous System），即 AS，是指一组通过统一的路由政策或路由协议互相交换路由信息的网络。在这个 AS 中，所有的 OSPF 路由器都维护一个相同的数据库。该数据库中存放的是路由域中相应链路的状态信息，OSPF 路由器正是通过这个数据库计算出其 OSPF 路由表的。作为一种链路状态的路由协议，OSPF 将 LSA（Link State Advertisement，链路状态广告）包传送给在某一区域内的所有路由器。这一点与距离矢量路由协议不同，因为运行距离矢量路由协议的路由器是将部分或全部的路由表传递给与其相邻的路由器。

SPF 算法是 OSPF 路由协议的基础。SPF 算法有时也被称为 Dijkstra 算法，这是因为最短路径优先算法 SPF 是 Dijkstra 发明的。SPF 算法将每一个路由器作为根（ROOT）来计算其到每一个目的地路由器的距离，每一个路由器根据一个统一的数据库会计算出路由域的拓扑结构图，该结构图类似于一棵树，在 SPF 算法中，被称为最短路径树。在 OSPF 路由协议中，最短路径树的树干长度，即 OSPF 路由器至每一个目的地路由器的距离，称为 OSPF 的 Cost，其算法为：Cost = 100×106/链路带宽。在这里，链路带宽以 b/s 来表示。也就是说，OSPF 的 Cost 与链路的带宽成反比，带宽越高，Cost 越小，表示 OSPF 到目的地的距离越近。例如，FDDI 或快速以太网的 Cost 为 1，2M 串行链路的 Cost 为 48，10M 以太网的 Cost 为 10 等。

作为一种典型的链路状态的路由协议，OSPF 协议还遵循链路状态路由协议的统一算法。链路状态的算法非常简单，主要包括以下三大步骤：

（1）当路由器初始化或当网络结构发生变化（例如增减路由器、链路状态发生变化等）时，路由器会产生 LSA 包，该数据包里包含路由器上的所有相连链路，也就是所有端口的状态信息。

（2）区域内的所有相邻路由器都将接收这个广告包。相邻路由器根据其接收到的链路状态信息更新自己的数据库，并将该链路状态信息转送给与其相邻的路由器，直至稳定的一个过程。

（3）当网络重新收敛后，所有的路由器会根据其各自的链路状态信息数据库计算出各自的路由表。该路由表中包含路由器到每一个可到达目的地的 Cost（开销）以及到达该目的地所要转发的下一个路由器（next-hop，下一跳）。

OSPF 同时也是一种内部网关协议，设计用于扩展 IP 网络，支持 IP 子网划分和路由信息外部导出标记。OSPF 也允许在发送和接收包时进行包认证和使用 IP 多播，思科设备支持 RFC 1253——

OSPF 管理信息库（Management Information Base，MIB），具有以下特征的 OSPF v2：

- 支持残余区域定义。
- 通过任何 IP 路由协议学习到的路由可以被再分布在其他 IP 路由协议上。在内部域级别上，意味着 OSPF 可以导入通过 EIGRP 和 RIP 学习到的路由。OSPF 也可以导出到 RIP 协议中使用。
- 支持在一个区域内在邻居路由器间采用纯文本和 MD5 身份认证。
- 配置路由接口参数，包括接口输出开销、重发间隔、接口传输延时、路由器优先级、路由器死亡和 hello 消息发送间隔，以及身份认证密钥。
- 支持虚拟链接。
- 支持非纯 stub 区域（Not so stubby area，NSSA）。

因为有关 OSPF 协议的工作原理在笔者编著的《网管员必读——网络基础》（第二版）中已有详细介绍，所以在此不再赘述。

【说明】OSPF 通常需要在许多 IR（Internal Router，内部路由器，是指在同一个 OSPF 区域中的所有路由器）间协同工作，区域边界路由器（Area Border Router，ABR）连接到多个区域和自治系统边界路由器（Autonomous System Boundary Router，ASBR，也称“AS 边界路由器”）。最基本的 OPSF 配置是全部使用默认参数值：无身份认证、接口指派到区域。如果要自定义 OSPF 网络环境，则必须确保所有路由器的配置协调一致。

5.7.2　启用 OSPF

与其他路由协议一样，要启用 OSPF，首先需要创建一个 OSPF 路由进程，指定与路由进程相关联的 IP 地址范围，分配与 IP 地址范围相关联的区域 ID。这些任务可以自全局配置模式开始，通过表 5-40 所示的步骤完成。

表 5-40　启用 OSPF 的步骤

步骤	命令	用途说明
1	Router(config)# **router ospf** *process-id*	启用 OSPF 路由进程（参数 *process-id* 用于指定 OSPF 路由进程 ID），并进入路由器配置模式
2	Router(config-router)# **network** *ip-address wildcard-mask* **area** *area-id*	通过指定 IP 地址和通配符掩码来定义一个运行 OSPF 路由协议的接口（也就是指定使用 OSPF 协议的网络），并为该接口定义一个区域 ID，也就是把它分配到一个指定的区域中

5.7.3　配置 OSPF 接口参数

OSPF 允许根据需要改变某个指定接口的 OSPF 参数，尽管这不是必须的，但是一些接口参数必须与同一网络中其他路由器的配置一致。这些参数可以由 **ip ospf hello-interval**, **ip ospf dead-interval** 或者 **ip ospf authentication-key** 接口配置命令配置。所以，确保如果你配置这些参数的任意一个，则一定要与网络中的其他路由器保持一致。

OSPF 接口参数的配置方法是采用如表 5-41 所示的接口配置模式命令。

表 5-41　OSPF 接口参数配置命令

命令	用途说明
Router(config-if)# **ip ospf cost** *cost*	指定 OSPF 接口发送数据包的开销
Router(config-if)# **ip ospf retransmit-interval** *seconds*	指定 OSPF 接口重传 LSA 广告包的时间间隔
Router(config-if)# **ip ospf transmit-delay** *seconds*	设定在 OSPF 接口上发送链路状态更新包所需的传输延时（也就是传输时间）
Router(config-if)# **ip ospf priority** *number-value*	设置 OSPF 接口优先级，以帮助确定一个网络中的指定路由器

续表

命令	用途说明
Router(config-if)# **ip ospf hello-interval** *seconds*	指定 OSPF 接口发送 Hello 消息包的时间间隔
Router(config-if)# **ip ospf dead-interval** *seconds*	设置因没有接收到某邻居设备的 hello 包而宣告邻居 OSPF 路由器关闭前所需等待的时间
Router(config-if)# **ip ospf authentication-key** *key*	分配一个由同一网段中邻居 OSPF 路由器访问本 OSPF 接口时用于进行简单身份认证的密码
Router(config-if)# **ip ospf message-digest-key** *key-id* **md5** *key*	启用 MD5 身份认证。这里的 *key-id* 和 *key* 参数值必须与同一网段中邻居路由器上的配置一致
Router(config-if)# **ip ospf authentication** [**message-digest** | **null**]	指定接口所用的身份认证类型

5.7.4 配置 OSPF 区域参数

OSPF 允许配置多个区域参数，其中包括指定身份认证类型、定义 stub（存根）区域、分配指定的开销到默认汇总路由中。在身份认证配置中，允许使用基于密码的保护，阻止对区域的非法访问。

Stub 区域是一个外部路由信息不能到达的区域，是用一个由区域边界路由器（ABR）产生的默认外部路由为自治系统外部目标指向 stub 区域的。要支持 OSPF stub 区域，必须在 stub 区域中使用默认路由。为了进一步减少发送到 stub 区域中的 LSA 包的数量，可以在 ABR 的 **area stub** 路由器配置模式命令中选择 **no-summary** 关键字，以阻止 ABR 发送 LSA 广告包到 stub 区域。

要为网络指定区域参数，请用表 5-42 所示的路由器配置模式命令。

表 5-42 OSPF 区域参数配置命令

命令	用途说明
Router(config-router)# **area** *area-id* **authentication**	为 OSPF 区域启用身份认证
Router(config-router)# **area** *area-id* **authentication message-digest**	为 OSPF 区域启用 MD5 身份认证
Router(config-router)# **area** *area-id* **stub** [**no-summary**]	定义一个区域为 stub 区域
Router(config-router)# **area** *area-id* **default-cost** *cost*	分配一个指定的开销到用于 stub 区域的默认汇总路由

5.7.5 配置 OSPF NSSA

OSPF NSSA（not-so-stubby area，非纯 stub 区域）功能是在 RFC 1587 中描述的，是从 Cisco IOS 11.2 版本开始支持的。OSPF NSSA 是以前 OSPF stub 区域功能的扩展。

NSSA 可用于当你是一个 ISP 或者是一个必须连接到正在使用 OSPF 的中心站点的管理员对一个使用不同路由协议的远程站点进行简单管理。

要使用 NSSA，在公司的站点边界路由器和远程站点边界路由器之间不能运行 OSPF stub 区域，因为这样，远程站点的路由信息不能分布到 stub 区域，而要实现通信，两个站点的路由协议又需要维护。通过 NSSA，可以扩展 OSPF，以便通过定义公司站点路由器和远程站点路由器为一个 NSSA 区域来恢复远程连接。

与 OSPF stub 区域一样，NSSA 区域中也不能流入类型 5 的 LSA 广告包。仅在指定的 LSA 广告类型是 NSSA 区域中唯一可存在类型 7 时，路由可能会重新划分到一个 NSSA 区域中。NSSA 自治系统边界路由器（ASBR）产生类型 7 LSA 广告，以便路由可以被重新分配，而 NSSA 边界路由器（ABR）转换类型 7 LSA 广告包为类型 5 LSA 广告包，只有这样，才能在整个 OSPF 路由域中传播。在转换过程中，消息汇总和过滤都是允许的。

图 5-13 所示为一个 OSPF 区域 1 为 stub 区域的网络示例。EIGRP（Enhanced Interior Gateway Routing Protocol，增强型内部网关路由协议）路由不能传播到这个 OSPF 域，因为在 stub 区域中是不允许重新分配路由的。但是，一旦 OSPF 区域 1 定义为 NSSA 区域，NSSA ASBR 路由器通过产

生类型 7 LSA 广告包使得 EIGRP 路由可以流入到 OSPF NSSA 区域中。这种来自 RIP 路由器重新分配的路由将允许进入 OSPF 区域 1 中，因为 NSSA 是 stub 区域的扩展，原来 stub 区域的特性仍然存在，包括类型 5 LSA 广告包的操作。

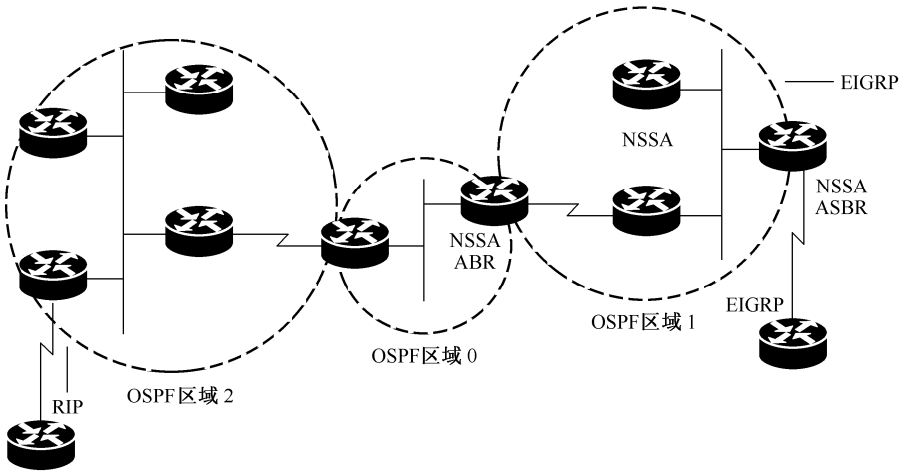

图 5-13　OSPF NSSA 区域示例

要按实际需求指定区域参数来配置 OSPF NSSA，可以使用 **area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate**]命令在路由器配置模式下定义一个区域成为 NSSA 区域。其中的参数说明如表 5-43 所示。

表 5-43　**area nssa** 命令参数说明

参数	功能说明
area-id	指定 NSSA 区域号，可以是十进制或者一个 IP 地址
no-redistribution	（可选）在路由器是一台 NSSA 区域 ABR 路由器时使用，使得仅导入重新分配路由到普通区域，不进入 NSSA 区域
default-information-originate	（可选）用于产生默认流入 NSSA 区域的类型 7 LSA 广告，仅影响 NSSA ABR 或者 NSSA ASBR 路由器

以下示例显示了如何标识区域 1 为一个 NSSA 区域。

```
Router(config)#router ospf 1    !--OSPF 进程 1
!--重新分配所有子网中的 RIP 路由，如果不带 subnets 关键字，则仅重新分配指定网络的路由，而不重新分配子网的路由
Router(config-router)#redistribute rip subnets
!--在由 IP 地址为 172.19.92.0、通配符掩码为 0.0.0.255 决定的范围（172.19.92.0/24）上启用 OSPF 动态路由协议，并分配为区域 1
Router(config-router)#network 172.19.92.0 0.0.0.255 area 1
Router(config-router)#area 1 nssa    !--把区域 1 标识为 NSSA 区域
```

要控制类型 7 LSA 汇总和过滤成为类型 5 LSA，可以在 ASBR 路由器上使用 **summary address** *prefix mask* [**not advertise**] [**tag** *tag*]路由器配置模式命令控制在类型转换过程中的汇总和过滤。命令中的参数说明如表 5-44 所示。

表 5-44　summary address 命令参数说明

参数	功能说明
ip-address	为地址范围指定汇总地址
mask	用于汇总路由的 IP 子网掩码
prefix	指定的汇总地址前缀
not-advertise	（可选）阻止广告与指定的 prefix/mask 参数对匹配的路由
tag tag	（可选）用于控制通过路由地图重新分配路由的标记值

在以下示例中，汇总地址 10.1.0.0 包括了 10.1.1.0、10.1.2.0 和 10.1.3.0 等。这样，在外部链路状态广告中仅需广告 10.1.0.0 这个地址了。

```
Router(config-router)#summary-address 10.1.0.0 255.255.0.0
```

5.7.6 在 OSPF 区域中配置路由汇总

路由汇总是广告的路由地址的合并，与本章前面介绍的 RIP 路由汇总一样，就是把多条分支路由通过 VLSM 方法汇总成一条总的路由，以减少路由器中的路由条目数，提高路由查询效率。这一功能可以使单一汇总路由通过 ABR 路由器广告到其他区域，广告的效率也更高，占用资源也更少。在 OSPF 中，ABR 路由器会通过路由广告把一个区域中的网络广告到其他区域中。如果一个区域中的网络号是采用像连续分配这种方式分配的，则可以配置 ABR 路由器广告一个汇总路由，覆盖属于指定范围区域内的所有个别网络。

要指定一个用于广告单一路由的地址范围，可以使用 **area** *area-id* **range** *ip-address mask* [**advertise** | **not-advertise**][**cost** *cost*]路由器配置命令，其中的参数说明如表 5-45 所示。

表 5-45 **area range** 命令参数说明

参数	功能说明
area-id	要汇总路由的区域标识，也可以是一个十进制或者一个 IP 地址
ip-address	要被汇总的路由的 IP 地址
ip-address-mask	要被汇总的路由的子网掩码
advertise	（可选）设置地址范围为允许广告状态，产生类型 3 的汇总 LSA
not-advertise	（可选）设置地址范围为禁止广告状态。类型 3 LSA 被取消，分支网络间相互不可见
cost cost	（可选）指定汇总路由的开销（度量，跳数），用 OSPF 的 SPF 路由算法来计算确定到达目标的最短路径，取值范围是 0～16777215

以下示例是指定了一个由 ABR 路由器向 10.0.0.0 网络中的其他所有子网区域和所有在 192.168.110.0 网络中的主机广告汇总路由。

```
Router(config)#interface ethernet 0
Router(config-if)#ip address 192.168.110.201 255.255.255.0
!
Router(config)#interface ethernet 1
Router(config-if)#ip address 192.168.120.201 255.255.255.0
!
Router(config-if)#router ospf 201
Router(config-if)#network 192.168.110.0 0.0.0.255 area 0
Router(config-if)#area 10.0.0.0 range 10.0.0.0 255.0.0.0
Router(config-if)#area 0 range 192.168.110.0 255.255.0.0
```

在从其他动态路由协议（如 RIP）中重新分配路由到 OSPF 时需要重新配置路由汇总。

要使软件为由一个网络地址和掩码覆盖的所有重新分配的路由汇总成一条汇总路由进行广告，可以使用 **summary-address** {{*ip-address mask*} | {*prefix mask*}} [**not-advertise**][**tag** *tag*]路由器配置模式命令，以便只有一条汇总路由被广告。使用 **not-advertise** 关键字来进行路由过滤。命令中的参数参见表 5-45。

5.7.7 创建 OSPF 虚拟链接

在 OSPF 中，所有区域必须与骨干区域连接。如果骨干连接中断或者骨干区域被重新划分，可以建立一个虚拟链接（Virtual Link）。虚拟链接的两个端点是 ABR 路由器。虚拟链路必须在两个 ABR 路由器上分别配置。每个路由器的这些配置信息是由其他虚拟端点（也就是其他 ABR 路由器）和两路由器所处的公共非骨干区域（也称为“过渡区域”）。但是虚拟链接不能穿过 stub 区域。

要建立虚拟链接，可以使用 **area** *area-id* **virtual-link** *router-id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval**

seconds] [[**authentication-key** *key*] | [**message-digest-key** *key-id* **md5** *key*]]路由器配置模式命令，其中的命令参数说明如表 5-46 所示。

表 5-46　area virtual-link 命令的参数说明

参数	功能说明
area-id	为虚拟链接指定过渡区域的区域号。也可以是一个十进制或者 IP 地址，没有默认值
router-id	与虚拟链接邻居关联的路由器 ID。可以通过 **show ip ospf** 命令查看。这个参数也没有默认值
hello-interval seconds	（可选）指定 hello 消息包发送的时间间隔，是一个无符号数。网络中所有路由器的此参数值均应一致，默认为 10 秒
retransmit-interval seconds	（可选）指定 LSA 包重发间隔，默认为 5 秒
transmit-delay seconds	（可选）指定接口上的更新包传输延时，默认为 1 秒
dead-interval seconds	（可选）指定在邻居路由器宣告某路由器关闭前，不能接收 hello 消息包的时间
ttl-security hops hop-count	（可选）在虚拟链路上配置 TTL 安全。hop-count 参数的取取值范围是 1～254

以下是一个以所有参数的默认值来创建一条虚拟链路的示例。

```
Router(config)#ip router ospf 1     !--启动 OSPF 进程 1
Router(config-if)#log-adjacency-changes     !--设置当发现邻居运行 OSPF 协议的设备关闭或者启动时发送一条系统日志
Router(config-if)#area 1 virtual-link 192.168.255.1    !--在 IP 地址为 192.168.255.1 的路由器上创建一个过渡区域为 1 的虚拟链接
```

要显示虚拟链接信息，可以使用 **show ip ospf virtual-links** 特权模式命令；要显示 OSPF 路由器的路由器 ID，则可以使用 **show ip ospf** 特权模式命令。

5.7.8　产生默认路由

可以强制 ASBR 路由器在 OSPF 路由表中产生一条默认路由。当指定要配置重新分配的路由到 OSPF 路由域时，路由器会自动成为 ABSR 路由器。但是，即使是 ASBR 路由器也不会默认产生一条默认路由到 OSPF 路由域中。要强制 ASBR 路由器产生一条默认路由，可以使用 **default-information originate** [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-name*]路由器配置模式命令。其中的参数说明如表 5-47 所示。

表 5-47　default-information originate 命令的参数说明

参数	功能说明
always	（可选）指定无论 OSPF 是否存在默认路由，总是广告默认路由
metric metric-value	（可选）指定用于默认路由的度量。如果选择这个参数，也不用“**default-metric**”路由器配置模式命令指定一个值，则默认度量值为 10
metric-type type-value	（可选）指定与广告进入 OSPF 路由域的默认路由关联的外部链路类型，可以是以下取值： ● 1：类型 1 外部路由 ● 2：类型 2 外部路由 默认是类型 2 外部路由
route-map map-name	（可选）为 OSPF 路由进程将产生的默认路由定义一个路由地图名