

目 录

第 1 章 IPv4 组播协议.....	1-1
1.1 IPv4 组播协议概述.....	1-1
1.1.1 组播简介	1-1
1.1.2 组播地址	1-1
1.1.3 IP组播报文转发	1-2
1.1.4 IP组播应用	1-3
1.2 PIM-DM	1-3
1.2.1 PIM-DM介绍	1-3
1.2.2 PIM-DM配置任务序列	1-4
1.2.3 PIM-DM典型案例.....	1-6
1.2.4 PIM-DM排错帮助.....	1-7
1.3 PIM-SM.....	1-7
1.3.1 PIM-SM介绍	1-7
1.3.2 PIM-SM配置任务序列	1-9
1.3.3 PIM-SM典型案例.....	1-12
1.3.4 PIM-SM排错帮助.....	1-14
1.4 MSDP配置	1-14
1.4.1 MSDP介绍.....	1-14
1.4.2 MSDP配置任务简介	1-15
1.4.3 配置MSDP基本功能	1-16
1.4.4 配置MSDP对等体.....	1-17
1.4.5 配置报文收发.....	1-17
1.4.6 配置SA-cache参数	1-18
1.4.7 MSDP举例.....	1-18
1.4.8 MSDP排错帮助	1-24
1.5 ANYCAST RP配置	1-25
1.5.1 ANYCAST RP介绍.....	1-25
1.5.2 ANYCAST RP配置任务	1-25
1.5.3 ANYCAST RP典型案例	1-27
1.5.4 ANYCAST RP排错帮助	1-29
1.6 PIM-SSM	1-29
1.6.1 PIM-SSM 介绍.....	1-29
1.6.2 PIM-SSM 配置任务序列	1-30
1.6.3 PIM-SSM 典型案例	1-30
1.6.4 PIM-SSM 排错帮助	1-32

1.7 DVMRP.....	1-32
1.7.1 DVMRP介绍	1-32
1.7.2 配置任务序列.....	1-33
1.7.3 DVMRP典型案例.....	1-34
1.7.4 DVMRP排错帮助.....	1-35
1.8 DCSCM	1-36
1.8.1 DCSCM介绍	1-36
1.8.2 DCSCM配置任务序列	1-36
1.8.3 DCSCM典型案例.....	1-40
1.8.4 DCSCM排错帮助.....	1-41
1.9 IGMP	1-41
1.9.1 IGMP介绍	1-41
1.9.2 配置任务序列.....	1-42
1.9.3 IGMP典型案例.....	1-44
1.9.4 IGMP排错帮助.....	1-45
1.10 IGMP Snooping配置.....	1-46
1.10.1 IGMP Snooping介绍	1-46
1.10.2 IGMP Snooping配置任务	1-46
1.10.3 IGMP Snooping典型案例.....	1-48
1.10.4 IGMP Snooping排错帮助.....	1-51
1.11 IGMP Proxy配置.....	1-52
1.11.1 IGMP Proxy介绍	1-52
1.11.2 IGMP Proxy配置任务.....	1-52
1.11.3 IGMP Proxy举例	1-53
1.11.4 IGMP Proxy排错帮助.....	1-56
第 2 章 IPv6 组播协议.....	2-1
2.1 PIM-DM6	2-1
2.1.1 PIM-DM6 介绍	2-1
2.1.2 PIM-DM6 配置任务序列	2-2
2.1.3 PIM-DM6 典型案例.....	2-4
2.1.4 PIM-DM6 排错帮助.....	2-5
2.2 PIM-SM6.....	2-5
2.2.1 PIM-SM6 介绍	2-5
2.2.2 PIM-SM6 配置任务序列	2-7
2.2.3 PIM-SM6 典型案例.....	2-10
2.2.4 PIM-SM6 排错帮助.....	2-12
2.3 ANYCAST RP v6 配置	2-13

2.3.1 ANYCAST RP v6 介绍.....	2-13
2.3.2 ANYCAST RP v6 配置任务	2-13
2.3.3 ANYCAST RP v6 典型案例	2-15
2.3.4 ANYCAST RP v6 排错帮助	2-17
2.4 PIM-SSM6	2-17
2.4.1 PIM-SSM6 介绍.....	2-17
2.4.2 PIM-SSM6 配置任务序列	2-17
2.4.3 PIM-SSM6 典型案例	2-18
2.4.4 PIM-SSM6 排错帮助	2-20
2.5 IPv6 DCSCM	2-20
2.5.1 IPv6 DCSCM介绍	2-20
2.5.2 IPv6 DCSCM配置任务序列.....	2-21
2.5.3 IPv6 DCSCM典型案例	2-23
2.5.4 IPv6 DCSCM排错帮助	2-24
2.6 MLD.....	2-24
2.6.1 MLD介绍	2-24
2.6.2 MLD配置任务序列.....	2-24
2.6.3 MLD典型案例	2-27
2.6.4 MLD排错帮助	2-28
2.7 MLD Snooping	2-28
2.7.1 MLD Snooping介绍.....	2-28
2.7.2 MLD Snooping配置任务	2-28
2.7.3 MLD Snooping典型案例	2-30
2.7.4 MLD Snooping排错帮助	2-33
第 3 章 组播VLAN配置	3-1
3.1 组播VLAN介绍.....	3-1
3.2 组播 VLAN配置任务.....	3-1
3.3 组播VLAN举例.....	3-2

第1章 IPv4 组播协议

1.1 IPv4 组播协议概述

本章对IPv4组播协议的配置进行介绍。

1.1.1 组播简介

当信息（包括数据、语音和视频）传送的目的地是网络中的少数用户时，可以采用多种传送方式。可以采用单播（Unicast）的方式，即为每个用户单独建立一条数据传送通路；或者采用广播（Broadcast）的方式，把信息传送给网络中的所有用户，不管他们是否需要，都会接收到广播来的信息。例如，在一个网络上有200个用户需要接收相同的信息时，传统的解决方案是用单播方式把这一信息分别发送200次，以便确保需要数据的用户能够得到所需的数据；或者采用广播的方式，在整个网络范围内传送数据，需要这些数据的用户可直接在网络上获取。这两种方式都浪费了大量宝贵的带宽资源，而且广播方式也不利于信息的安全和保密。

IP组播技术的出现及时解决了这个问题。组播源仅发送一次信息，组播路由协议为组播数据包建立树型路由，被传递的信息在尽可能远的分叉路口才开始复制和分发，因此，信息能够被准确高效地传送到每个需要它的用户。

需要注意的是，组播源不一定需要加入组播组，它向某些组播组发送数据，自己不一定是该组的接收者。可以同时有多个源向一个组播组发送报文。网络中可能有不支持组播的路由器，组播路由器可以使用隧道方式将组播包封装在单播IP包中传送给相邻的组播路由器，相邻的组播路由器再将单播IP头剥掉，然后继续进行组播传输。从而避免对网络的结构进行较大的改动。组播的优势主要在于：

- 1) 提高效率：降低网络流量，减轻服务器和CPU负荷；
- 2) 优化性能：减少冗余流量；
- 3) 分布式应用：使多点应用成为可能。

1.1.2 组播地址

组播报文的目的地地址使用D类IP地址，范围是从224.0.0.0到239.255.255.255。D类地址不能出现在IP报文的源IP地址字段。单播数据传输过程中，一个数据包传输的路径是从源地址路由到目的地址，利用“逐跳”（hop-by-hop）的原理在IP网络中传输。然而在IP组播环境中，数据包的目的地址不是一个，而是一组，形成组地址。所有的信息接收者都加入到一个组内，并且一旦加入之后，流向组地址的数据立即开始向接收者传输，组中的所有成员都能接收到数据包。组播组中的成员是动态的，主机可以在任何时刻加入和离开组播组。

组播组可以是永久的也可以是临时的。组播组地址中，有一部分由官方分配的，称为永久组播组。永久组播组保持不变的是它的IP地址，组中的成员构成可以发生变化。永久组播组中成员的数量都可以是任意的，甚至可以为零。那些没有保留下来供永久组播组使用的IP组播地址，可以被临时组播组利用。

224.0.0.0~224.0.0.255为预留的组播地址（永久组地址），地址224.0.0.0保留不做分配，其它地址供路由协议使用； 224.0.1.0~238.255.255.255为用户可用的组播地址（临时组地址），全网范围内有效；239.0.0.0~239.255.255.255为本地管理组播地址，仅在特定的本地范围内有效。常用的预留组播地址列表如下：

- 224.0.0.0 基准地址（保留）
- 224.0.0.1 所有主机的地址
- 224.0.0.2 所有组播路由器的地址
- 224.0.0.3 不分配
- 224.0.0.4 DVMRP 路由器
- 224.0.0.5 OSPF 路由器
- 224.0.0.6 OSPF DR
- 224.0.0.7 ST 路由器
- 224.0.0.8 ST 主机
- 224.0.0.9 RIP-2 路由器
- 224.0.0.10 IGRP 路由器
- 224.0.0.11 活动代理
- 224.0.0.12 DHCP 服务器/中继代理
- 224.0.0.13 所有PIM 路由器
- 224.0.0.14 RSVP 封装
- 224.0.0.15 所有CBT 路由器
- 224.0.0.16 指定SBM
- 224.0.0.17 所有SBMS
- 224.0.0.18 VRRP
- 224.0.0.22 IGMP

以太网传输单播IP报文的时候，目的MAC地址使用的是接收者的MAC地址。但是在传输组播报文时，传输目的不再是一个具体的接收者，而是一个成员不确定的组，所以使用的是组播MAC地址。组播MAC地址是和组播IP地址对应的。IANA（Internet Assigned Number Authority）规定，组播MAC地址的高25bit为0x01005e，MAC 地址的低23bit为组播IP地址的低23bit。

由于IP组播地址的后28位中只有23位被映射到MAC地址，这样就会有32个IP组播地址映射到同一MAC地址上。

1.1.3 IP组播报文转发

在组播模型中，源主机向IP数据包目的地址字段内的组播组地址所表示的主机组传送信

息。和单播模型不同的是，组播模型必须将组播数据包转发到多个外部接口上以便能传送到所有接收站点，因此组播转发过程比单播转发过程更加复杂。

为了保证组播信息包都是通过最短路径到达路由器，组播必须依靠单播路由表或者单独提供给组播使用的单播路由表（如DVMRP路由），对组播信息包的接收接口进行一定的检查，这种检查机制就是大部分组播路由协议进行组播转发的基础——RPF（Reverse Path Forwarding，逆向路径转发）检查。组播路由器利用到达的组播数据包的源地址来查询单播路由表或者独立的组播路由表，以确定此数据包到达的入接口处于接收站点至源地址的最短路径上。如果使用的是有源树，这个源地址就是发送组播数据包的源主机的地址；如果使用的是共享树，该源地址就是共享树的根的地址。当组播数据包到达路由器时，如果RPF 检查通过，数据包则按照组播转发项进行转发，否则，数据包被丢弃。

1.1.4 IP组播应用

IP组播技术有效地解决了单点发送多点接收的问题，实现了IP网络中点到多点的高效数据传送，能够大量节约网络带宽、降低网络负载。利用网络的组播特性可以方便地提供一些新的增值业务。在线直播、网络电视、远程教育、远程医疗、网络电台、实时视/音频会议等互联网的信息服务领域可以提供如下应用：

- 1) 多媒体、流媒体的应用；
- 2) 数据仓库、金融应用（股票）等；
- 3) 任何“点到多点”的数据发布应用。

在 IP 网络中多媒体业务日渐增多的情况下，组播有着巨大的市场潜力，组播业务也将逐渐得到推广和普及。

1.2 PIM-DM

1.2.1 PIM-DM介绍

PIM-DM（Protocol Independent Multicast，Dense Mode，协议独立组播—密集模式）属于密集模式的组播路由协议，适用于小型网络，在这种网络环境下，组播组的成员相对比较密集。

PIM-DM 的工作过程可以概括为：邻居发现、扩散—剪枝过程、嫁接阶段。

1. 邻居发现

PIM-DM 路由器刚开始启动时，需要使用Hello报文来发现邻居。运行PIM-DM的各网络节点之间使用Hello报文保持联系。PIM-DM Hello报文是周期性发送的。

2. 扩散—剪枝过程（Flooding&Prune）

PIM-DM 假设网络上的所有主机都准备接收组播数据。当某组播源S开始向组播组G发送数据时，在路由器接收到组播报文后，首先根据单播路由表进行RPF检查，如果检查通过，路由器创建一个（S，G）表项，然后将组播报文向网络上所有下游PIM-DM节点转发

(Flooding)。如果没有通过RPF检查,即组播报文是从错误的接口输入,则将该报文丢弃。经过这个过程,在PIM-DM组播域内,每个节点都会创建一个(S, G)表项。如果下游节点没有组播组成员,则向上游节点发剪枝(Prune)消息,通知上游节点不用再转发该组播组数据。上游节点收到剪枝消息后,就将相应的接口从其组播转发表项(S, G)对应的输出接口列表中删除,这就建立了一个以源S为根的SPT(Shortest Path Tree, SPT)树。剪枝过程最先由叶子路由器发起。

3. RPF检查

PIM-DM采用RPF检查,利用现存的单播路由表构建一棵从数据源始发的组播转发树。当一个组播包到达时,路由器首先判断到达路径的正确性。如果到达接口是单播路由指示的通往组播源的接口,就认为这个组播包是从正确路径而来;否则,将组播包作为冗余报文丢弃。作为路径判断依据的单播路由信息可以来源于任何一种单播路由协议,如RIP、OSPF 等发现的路由信息,而不依赖于特定的单播路由协议。

4. Assert机制

如果处于一个LAN网段上的两台组播路由器A和B,各自有到组播源S的接收途径,它们在接收到组播源S发出的组播数据报文以后,都会向LAN上转发该组播报文,这时,下游节点组播路由器C就会收到两份相同的组播报文。路由器检测到这种情况后,需要通过Assert机制来选定一个唯一的转发者。通过发送Assert报文,选出一条最优的转发路径,如果两条或两条以上路径的优先级和开销相同,则选择IP地址大的节点作为该(S, G)项的上游邻居,由它负责该(S, G)组播报文的转发。

5. 嫁接(Graft)

当被剪枝的下游节点需要恢复到转发状态时,该节点使用嫁接报文通知上游节点恢复组播数据转发。

6. PIM-DM的状态刷新

为了减少PIM-DM周期性的扩散-剪枝,PIM-DM协议最新版本提供了一个选项(option),它将从组播源的第一跳路由器开始,周期性的向下面广播(S, G)状态刷新消息以完成状态刷新。当下游PIM路由器收到(S, G)状态刷新消息,它就将剪枝计时器复位,终止剪枝计时器超时,从而即保证了网络的时效性,避免了周期性的扩散-剪枝过程。

1.2.2 PIM-DM配置任务序列

- 1、 启动 PIM-DM (必须)
- 2、 配置静态组播表项 (可选)
- 3、 配置 PIM-DM 辅助参数 (可选)
 - a) 配置 PIM-DM hello 报文间隔时间
 - b) 配置 state-refresh 报文间隔时间
 - c) 配置边缘接口
 - d) 配置管理边界
- 4、 关闭 PIM-DM 协议

1. 启动 PIM-DM 协议

在三层交换机上运行 PIM-DM 路由协议的基本配置很简单，需全局配置模式下打开 PIM 组播开关，然后在相应接口下打开 PIM-DM 开关即可。

命令	解释
全局配置模式	
ip pim multicast-routing no ip pim multicast-routing	使各个接口上的 PIM-DM 协议进入使能状态（但真正在接口上开始 PIM-DM 协议，还需下面的命令）。

然后在接口上打开 PIM-SM 开关

命令	解释
接口配置模式	
ip pim dense-mode	启动本接口 PIM-DM 协议。（必须）

2. 配置静态组播表项

命令	解释
全局配置模式	
ip mroute <A.B.C.D> <A.B.C.D> <ifname> <ifname> no ip mroute <A.B.C.D> <A.B.C.D> [<ifname> <ifname>]	配置静态组播表项，其 no 命令删除静态组播表项或其出接口。

3. 配置 PIM-DM 辅助参数

a) 配置 PIM-DM hello 报文间隔时间

命令	解释
接口配置模式	
ip pim hello-interval <interval> no ip pim hello-interval	配置接口 PIM-DM hello 报文间隔时间；本命令的 no 操作恢复为缺省值。

b) 配置 state-refresh 报文间隔时间

命令	解释
全局配置模式	
ip pim state-refresh origination-interval no ip pim state-refresh origination-interval	全局模式下配置 PIM-DM state-refresh 报文间隔时间；本命令的 no 操作恢复为缺省值。

c) 配置边缘接口

命令	解释
接口配置模式	

ip pim bsr-border no ip pim bsr-border	配置接口为 PIM-DM 边缘接口，边缘接口上，BSR 相关消息不向该接口发送也不从该接口接收，连接的网络被认为都是该接口的直连网络。本命令的 no 操作取消该配置。
---	---

d) 配置管理边界

命令	解释
接口配置模式	
ip pim scope-border <1-99> <acl_name> no ip pim scope-border	配置 PIM-DM 管理边界和使用的 ACL。组播数据不向 SCOPE-BORDER 扩散，默认的情形下，认为 239.0.0.0/8 的范围为管理组范围，若配置了 ACL，则 ACL permit 的范围为管理组范围。本命令的 no 操作取消该配置。

4. 关闭 PIM-DM 协议

命令	解释
接口配置模式	
no ip pim dense-mode	在接口上关闭 PIM-DM 协议。
全局配置模式	
no ip pim multicast-routing	全局关闭 PIM-DM 协议。

1.2.3 PIM-DM典型案例

如下图，将 switchA，switchB 的以太网接口加入到相应的 VLAN 中，并在各 VLAN 接口上启动 PIM-DM 协议。如果 VLAN 内同时配置了 IGMP SNOOPING，则组播流量能精确到端口，而不在整个 VLAN 内泛洪。

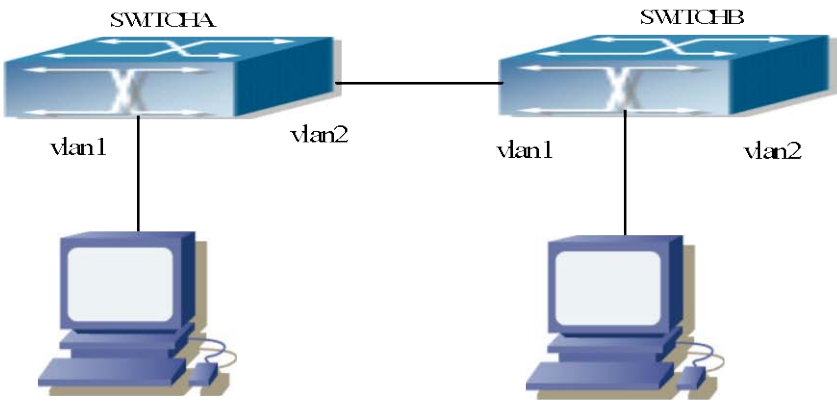


图 1-1 PIM-DM 典型环境

switchA 和switchB配置步骤如下：

(1) 配置SwitchA:

```
Switch (config)#ip pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)# ip address 10.1.1.1 255.255.255.0
Switch(Config-if-Vlan1)# ip pim dense-mode
Switch(Config-if-Vlan1)#exit
Switch (config)#interface vlan2
Switch(Config-if-Vlan2)# ip address 12.1.1.1 255.255.255.0
Switch(Config-if-Vlan2)# ip pim dense-mode
```

(2) 配置SwitchB:

```
Switch (config)#ip pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)# ip address 12.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)# ip pim dense-mode
Switch(Config-if-Vlan1)#exit
Switch (config)#interface vlan 2
Switch(Config-if-Vlan2)# ip address 20.1.1.1 255.255.255.0
Switch(Config-if-Vlan2)# ip pim dense-mode
```

同时要注意配置好单播路由协议，确保网络中各设备之间能够在网络层互通，并且能够借助单播路由协议实现动态路由更新。

1.2.4 PIM-DM排错帮助

在配置、使用 PIM-DM 协议时，可能会由于物理连接、配置错误等原因导致 PIM-DM 协议未能正常运行。因此，用户应注意以下要点：

- ☞ 应该保证物理连接的正确无误
- ☞ 保证接口和链路协议是 UP（使用 show interface 命令）
- ☞ 保证全局配置模式下打开 PIM 协议(使用 ip pim multicast-routing)
- ☞ 在接口上启动 PIM-DM 协议（使用 ip pim dense-mode 命令）
- ☞ 组播协议需使用单播路由进行 RPF 检查，因此必须首先确保单播路由的正确性

如果使用检查仍无法解决 PIM-DM 的问题，那么请使用 debug pim 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给本公司技术服务中心。

1.3 PIM-SM

1.3.1 PIM-SM介绍

PIM-SM（Protocol Independent Multicast，Sparse Mode）即与协议无关组播-稀疏模式，属于稀疏模式的组播路由协议，主要用于组成员分布相对分散、范围较广、大规模的网

络。与密集模式的扩散—剪枝不同，PIM-SM协议假定所有的主机都不需要接收组播数据包，只有主机明确指定需要时，PIM-SM路由器才向它转发组播数据包。

PIM-SM通过设置汇聚点RP（Rendezvous Point）和自举路由器BSR（Bootstrap Router），向所有PIM-SM路由器通告组播信息，并利用路由器的加入/剪枝信息，建立起基于RP的共享树RPT（RP-rooted shared tree）。从而减少数据报文和控制报文占用的网络带宽，降低路由器的处理开销。组播数据沿着共享树流到该组播组成员所在的网段，当数据流量达到一定程度，组播数据流可以切换到基于源的最短路径树SPT，以减少网络延迟。PIM-SM不依赖于特定的单播路由协议，而是使用现存的单播路由表进行RPF检查。

1. PIM-SM工作原理

PIM-SM的工作过程主要有：邻居发现、RP共享树（RPT）的生成、组播源注册、SPT切换等。其中，邻居发现机制与PIM-DM相同，这里不再介绍。

(1) RP共享树（RPT）的生成

当主机加入一个组播组G时，与该主机直接相连的叶子路由器通过IGMP报文了解到有组播组G的接收者，就为组播组G计算出对应的汇聚点RP，然后向朝着RP方向的上一级节点发送加入组播组的消息（join 消息）。从叶子路由器到RP之间途经的每个路由器都会在转发表中生成（*, G）表项，表示由任意源发出的，发送至组播组G的，都适用于该表项。当RP收到发往组播组G的报文后，报文就会沿着已经建立好的路径到达叶子路由器，进而到达主机。这样就生成了以RP为根的RPT。

(2) 组播源注册

当组播源S向组播组G发送了一个组播报文时，与其直接相连的PIM-SM组播路由器收到该报文以后，就负责将该组播报文封装成注册报文，单播给对应的RP。如果一个网段上有多个PIM-SM组播路由器，这时候将由指定路由器DR（Designated Router）负责发送该组播报文。

(3) SPT切换

当组播路由器发现从RP发来的目的地址为G的组播报文的速率超过了阈值时，组播路由器就向朝着源S的上一级节点发送加入消息，导致RPT向SPT的切换。

2. PIM-SM 配置前准备工作

(1) 配置候选RP

在PIM-SM网络中，可以存在多个RP（候选RP），每个候选RP（Candidate-RP，C-RP）负责转发目的地址在一定范围内的组播报文。配置多个候选RP可以实现RP负载分担。候选RP之间没有主次之分，所有的组播路由器收到BSR通告的候选RP消息后，根据相同的算法计算出与某一组播组对应的RP。

注意，一个RP可以为多个组播组服务，也可以为所有组播组服务。每个组播组在任意时刻，只能唯一地对应一个RP，不能同时对应多个RP。

(2) 配置BSR

BSR 是PIM-SM 网络里的管理核心，它负责收集候选RP发来的信息，并把它们广播出去。

一个网络内部只能有一个BSR，但可以配置多个候选BSR（Candidate-BSR，C-BSR）。

这样，一旦某个BSR发生故障后，能够切换到另外一个。C-BSR通过自动选举产生BSR。

1.3.2 PIM-SM配置任务序列

- 1、启动 PIM-SM（必须）
- 2、配置静态组播表项（可选）
- 3、配置 PIM-SM 辅助参数（可选）
 - (1) 配置 PIM-SM 接口参数
 - 1) 配置 PIM-SM hello 报文间隔时间
 - 2) 配置 PIM-SM hello 报文 holdtime 时间
 - 3) 配置 PIM-SM 邻居访问列表
 - 4) 配置接口为 PIM-SM 边缘接口
 - 5) 配置接口为 PIM-SM 管理边界
 - (2) 配置 PIM-SM 全局参数
 - 1) 配置交换机作为候选 BSR
 - 2) 配置交换机作为候选 RP
 - 3) 配置静态 RP
 - 4) 配置内核组播路由缓存时间
- 4、关闭 PIM-SM 协议

1. 启动 PIM-SM 协议

在三层交换机上运行 PIM-SM 路由协议的基本配置很简单，需全局配置模式下打开 PIM 组播开关，然后在相应接口下打开 PIM-SM 开关即可。

命令	解释
全局配置模式	
ip pim multicast-routing	使各个接口上的 PIM-SM 协议进入使能状态(但真正在接口上开始 PIM-SM 协议，还需下面的命令)。(必须)

然后在接口上打开 PIM-SM 开关

命令	解释
接口配置模式	
ip pim sparse-mode	启动本接口 PIM-SM 协议。(必须)

2. 配置静态组播表项

命令	解释
全局配置模式	
ip mroute <A.B.C.D> <A.B.C.D> <ifname> <.ifname> no ip mroute <A.B.C.D> <A.B.C.D> [<.ifname> <.ifname>]	配置静态组播表项，其 no 命令删除静态组播表项或其出接口。

3. 配置 PIM-SM 辅助参数

(1) 配置 PIM-SM 接口参数

1) 配置 PIM-SM hello 报文间隔时间

命令	解释
接口配置模式	
ip pim hello-interval < interval> no ip pim hello-interval	配置接口 PIM-SM hello 报文间隔时间；本命令的 no 操作恢复为缺省值。

2) 配置 PIM-SM hello 报文 holdtime 时间

命令	解释
接口配置模式	
ip pim hello-holdtime <value> no ip pim hello-holdtime	配置接口 PIM-SM hello 报文中的 holdtime 域的值；本命令的 no 操作恢复为缺省值。

3) 配置 PIM-SM 邻居访问列表

命令	解释
接口配置模式	
ip pim neighbor-filter {<access-list-number> } no ip pim neighbor-filter {<access-list-number> }	配置邻居访问列表。如果被列表过滤，如果已经同此邻居建立连接，则此连接马上被切断，如果没有建立连接，则这个连接不能建立。

4) 配置边缘接口

命令	解释
接口配置模式	
ip pim bsr-border no ip pim bsr-border	配置接口为 PIM-DM 边缘接口，边缘接口上，BSR 相关消息不向该接口发送也不从该接口接收，连接的网络被认为都是该接口的直连网络。本命令的 no 操作取消该配置。

5) 配置管理边界

命令	解释
接口配置模式	
ip pim scope-border <1-99> <acl_name> no ip pim scope-border	配置 PIM-DM 管理边界和使用的 ACL。组播数据不向 SCOPE-BORDER 扩散，默认的情形下，认为 239.0.0.0/8 的范围为管理组范围，若配置了 ACL，则 ACL permit 的范围为管理组范围。acl_name 应当是 IPV4 标准 ACL 名。本命令的 no 操作取消该配置。

(2) 配置 PIM-SM 全局参数

1) 配置交换机作为候选 BSR

命令	解释
全局配置模式	
ip pim bsr-candidate {vlan <vlan-id> <ifname>} [<mask-length>] [<priority>] no ip pim bsr-candidate	该命令为全局候选 BSR 配置命令，用于配置 PIM-SM 候选 BSR 的信息，以用于同其它候选 BSR 竞争 BSR 路由器；本命令的 no 操作为取消候选 BSR 的配置。

2) 配置交换机作为候选 RP

命令	解释
全局配置模式	
ip pim rp-candidate {vlan<vlan-id> loopback<index> <ifname>} [<A.B.C.D>] [<priority>] no ip pim rp-candidate	该命令为全局候选 RP 配置命令，用于配置 PIM-SM 候选 RP 的信息，以用于同其它候选 RP 竞争 RP 路由器；本命令的 no 操作为取消候选 RP 的配置。

3) 配置静态 RP

命令	解释
全局配置模式	
ip pim rp-address <A.B.C.D> [<A.B.C.D/M>] no ip pim rp-address <A.B.C.D> {<all/> <A.B.C.D/M>}	该命令为全局或某个组播地址范围的组播组配置静态 RP，本命令的 no 操作为取消静态 RP 的配置。

4) 配置内核组播路由缓存时间

命令	解释
全局配置模式	
ip multicast unresolved-cache aging-time <value> no ip multicast unresolved-cache aging-time	配置内核组播路由缓存时间；本命令的 no 操作恢复为缺省值。

4. 关闭 PIM-SM 协议

命令	解释
接口配置模式	
no ip pim sparse-mode no ip pim multicast-routing (全局配置模式)	关闭 PIM-SM 协议。

1.3.3 PIM-SM典型案例

如下图所示，将switchA，switchB，switchC，switchD的以太网接口加入到相应VLAN中，并在各VLAN接口上启动PIM-SM协议。如果VLAN内同时配置了IGMP SNOOPING，则组播流量能精确到端口，而不在整个VLAN内泛洪。

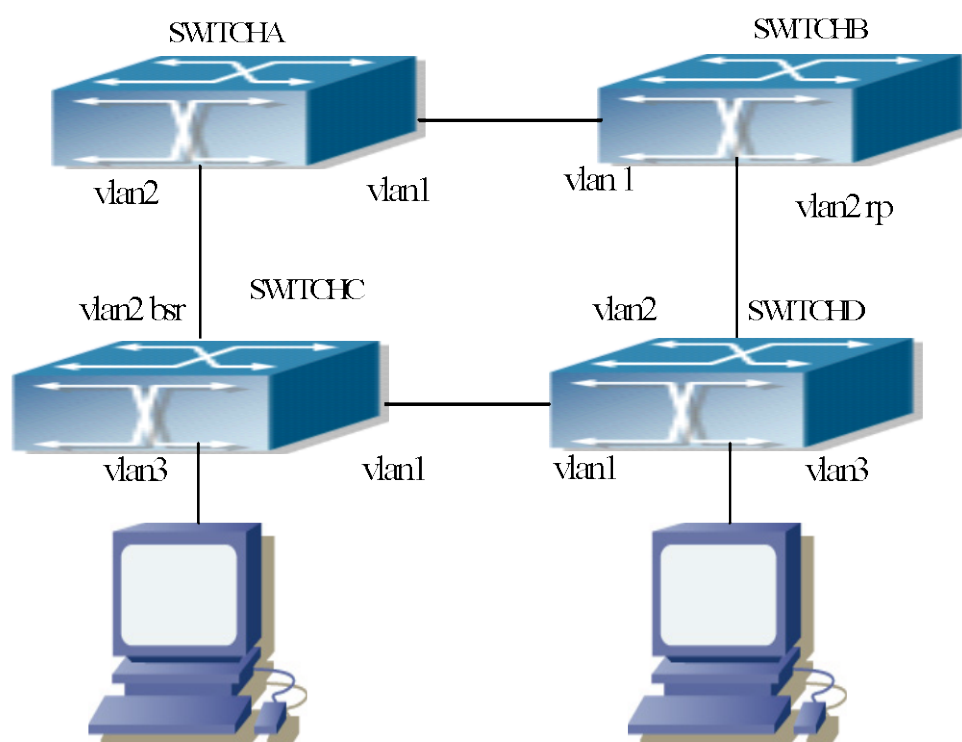


图 1-2 PIM-SM 典型环境

switchA 和 switchB，switchC，switchD 配置步骤如下：

(1) 配置 SwitchA:

```
Switch (config)#ip pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-If-Vlan1)# ip address 12.1.1.1 255.255.255.0
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (config)#interface vlan 2
Switch(Config-If-Vlan2)# ip address 13.1.1.1 255.255.255.0
Switch(Config-If-Vlan2)# ip pim sparse-mode
```

(2) 配置 SwitchB:

```
Switch (config)#ip pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-If-Vlan1)# ip address 12.1.1.2 255.255.255.0
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (config)#interface vlan 2
Switch(Config-If-Vlan2)# ip address 24.1.1.2 255.255.255.0
Switch(Config-If-Vlan2)# ip pim sparse-mode
Switch(Config-If-Vlan2)# exit
Switch (config)# ip pim rp-candidate vlan2
```

(3) 配置 SwitchC:

```
Switch (config)#ip pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-If-Vlan1)# ip address 34.1.1.3 255.255.255.0
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (config)#interface vlan 2
Switch(Config-If-Vlan2)# ip address 13.1.1.3 255.255.255.0
Switch(Config-If-Vlan2)# ip pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch (config)#interface vlan 3
Switch(Config-If-Vlan3)# ip address 30.1.1.1 255.255.255.0
Switch(Config-If-Vlan3)# ip pim sparse-mode
Switch(Config-If-Vlan3)# exit
Switch (config)# ip pim bsr-candidate vlan2 30 10
```

(4) 配置 SwitchD:

```
Switch (config)#ip pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-If-Vlan1)# ip address 34.1.1.4 255.255.255.0
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (config)#interface vlan 2
Switch(Config-If-Vlan2)# ip address 24.1.1.4 255.255.255.0
Switch(Config-If-Vlan2)# ip pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch (config)#interface vlan 3
Switch(Config-If-Vlan3)# ip address 40.1.1.1 255.255.255.0
Switch(Config-If-Vlan3)# ip pim sparse-mode
```

同时要注意配置好单播路由协议，确保网络中各设备之间能够在网络层互通，并且能够借助单播路由协议实现动态路由更新。

1.3.4 PIM-SM排错帮助

在配置、使用 PIM-SM 协议时，可能会由于物理连接、配置错误等原因导致 PIM-SM 协议未能正常运行。因此，用户应注意以下要点：

- ☞ 应该保证物理连接的正确无误；
- ☞ 保证接口和链路协议是 UP（使用 `show interface` 命令）；
- ☞ 保证全局配置模式下 PIM 协议打开（使用 `ip pim multicast-routing`）；
- ☞ 保证接口上配置 PIM-SM（使用 `ip pim sparse-mode`）；
- ☞ 组播协议需使用单播路由进行 RPF 检查，因此必须首先确保单播路由的正确性；
- ☞ PIM-SM 协议需要有 rp 和 bsr 的支持，所以首先使用 `show ip pim bsr-router`，看是否有 bsr 信息，如果不存在，则需要查看是否有通向 bsr 的单播路由；
- ☞ 使用 `show ip pim rp-hash` 命令查看 rp 信息是否正确，如果没有 rp 信息，也要检查单播路由。

如果使用检查仍无法解决 PIM-SM 的问题，那么请使用 `debug pim/ debug pim bsr` 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给本公司技术服务中心。

1.4 MSDP配置

1.4.1 MSDP介绍

MSDP (Multicast Source Discovery Protocol, 组播源发现协议) 用来发现其它 PIM-SM 域内的组播源信息。配置了 MSDP 对等体的 RP 将其域内的活动组播源信息通过 SA 消息通告给它的所有 MSDP 对等体，这样，一个 PIM-SM 域内的组播源信息就会被传递到另一个 PIM-SM 域。在 MSDP 里使用的是域间信源树而不是共享树，而且要求域内组播路由协议必须是 PIM-SM。

- PIM-SM 协议中 RP 工作原理

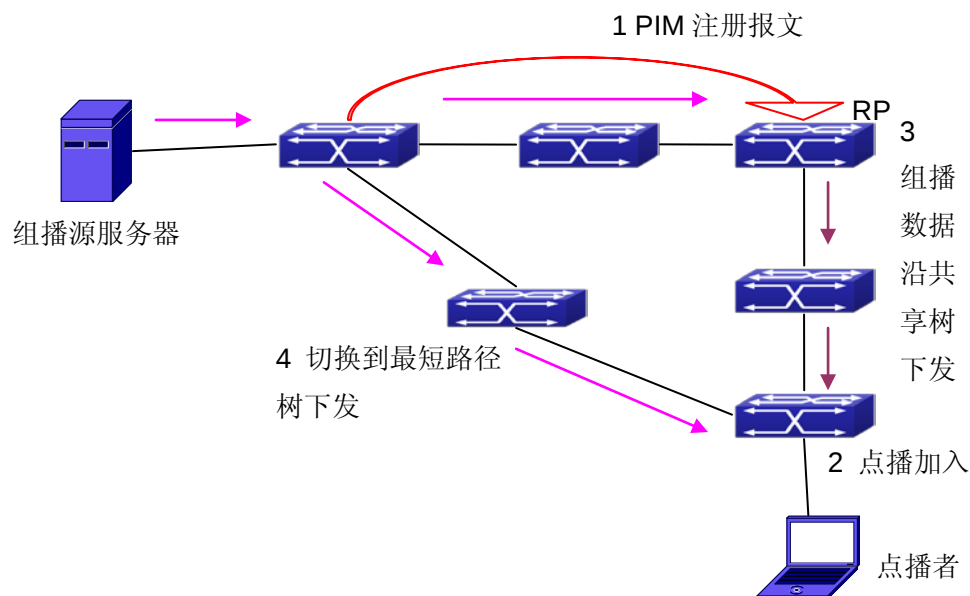


图 1-3 RP 工作原理

1.4.2 MSDP配置任务简介

1. 配置MSDP基本功能
 - 1) 使能MSDP(必选)
 - 2) 创建MSDP对等体(必选)
 - 3) 配置Connect-Source接口
 - 4) 配置静态RPF对等体
 - 5) 配置Originator-RP
 - 6) 配置TTL阈值
2. 配置MSDP对等体参数
 - 1) 配置Connect-Source接口
 - 2) 配置MSDP对等体的描述信息
 - 3) 配置AS号
 - 4) 配置MSDP全连接组
 - 5) 配置缓存最大数目
3. 配置报文收发参数
 - 1) 配置SA报文创建过滤策略
 - 2) 配置SA报文接收和转发过滤规则
 - 3) 配置SA请求报文
 - 4) 配置SA-Request报文过滤策略
4. 配置SA-cache参数
 - 1) 配置SA报文缓存

- 2) 配置缓存表项的存活时间
- 3) 配置缓存最大数目

1.4.3 配置MSDP基本功能

本节的所有命令都是在PIM-SM域内的RP上配置的，这些RP将成为MSDP对等体的一端。

1.4.3.1 配置准备

在配置MSDP基本功能之前，需完成以下任务：

- 配置任一单播路由协议，实现域内和域间网络层互通
- 配置PIM-SM基本功能，实现域内组播

在配置MSDP基本功能之前，需准备以下数据：

- MSDP对等体的IP地址
- 过滤策略列表

注意：MSDP不能和Any-cast RP一起使用，但是可以配置基于MSDP协议的Any-cast RP。

1.4.3.2 使能MSDP

在配置 MSDP 各功能之前，必须先使能 MSDP。

1.启动 MSDP 功能

2.配置 MSDP

1.启动 MSDP 功能

命令	解释
全局配置模式	
router msdp no router msdp	启动 MSDP 功能。no 命令关闭全局 MSDP 功能。

2.配置 MSDP 辅助参数

命令	解释
MSDP 配置模式	
connect-source <interface-type> <interface-number> no connect-source	配置 MSDP Peer 的 Connect-Source 接口。 no 命令取消配置的 Connect-Source 接口。
default-rpf-peer <peer-address> [rp-policy <acl-list-number> <word>] no default-rpf-peer	配置静态 RPF Peer。 no 命令取消配置的 RPF Peer。

originating-rp <interface-type> <interface-number> no originating-rp	配置 Originator-RP。 no 命令取消配置的 Originator-RP。
ttl-threshold <tvl> no ttl-threshold	配置 TTL 阈值。 no 命令取消配置的 TTL 阈值。

1.4.4 配置MSDP对等体

1.4.4.1 创建MSDP Peer

命令	解释
MSDP 配置模式	
peer <peer-address> no peer <peer-address>	创建 MSDP Peer。 no 命令删除 MSDP Peer。

1.4.4.2 配置MSDP 辅助参数

命令	解释
MSDP Peer 配置模式	
connect-source <interface-type> <interface-number> no connect-source	配置 MSDP Peer 的 Connect-Source 接口。 no 命令取消配置的 Connect-Source 接口。
description <text> no description	配置 MSDP 对等体的描述信息。 no 命令删除 MSDP 对等体的描述信息。
remote-as <as-num> no remote-as <as-num>	配置 MSDP Peer 的 AS 号。 no 命令取消配置 MSDP Peer 的 AS 号。
mesh-group <name> no mesh-group <name>	配置 MSDP Peer 加入指定全连接组。 no 命令取消配置 MSDP Peer 的全连接组成员身份。

1.4.5 配置报文收发

命令	解释
MSDP 配置模式	
redistribute [list <acl-list-number <acl-name>] no redistribute	配置 SA 报文创建过滤策略。 no 命令取消配置 SA 报文创建过滤策略。
MSDP 配置模式或 MSDP Peer 配置模式	

sa-filter (in out) [list <acl-number acl-name> rp-list <rp-acl-number rp-acl-name>] no sa-filter (in out) [[list <acl-number acl-name> rp-list <rp-acl-number rp-acl-name>]	配置 SA 报文接收和转发过滤规则。 no 命令取消配置的 SA 报文接收和转发过滤规则。
MSDP Peer 配置模式	
sa-request no sa-request	配置发送 SA 请求报文。 no 命令取消发送 SA 请求报文。
MSDP 配置模式	
sa-request-filter [list <access-list-number access-list-name>] no sa-request-filter [list <access-list-number access-list-name>]	配置 SA-Request 报文过滤策略。 取消配置 SA-Request 报文过滤策略。

1.4.6 配置SA-cache参数

命令	解释
MSDP 配置模式	
cache-sa-state no cache-sa-state	使能 SA 报文缓存。 关闭 SA 报文缓存。
cache-sa-holdtime <150-3600> no cache-sa-holdtime	配置缓存表项的存活时间。 恢复缓存表项的默认的存活时间。
MSDP 配置模式或 MSDP Peer 配置模式	
cache-sa-maximum <sa-limit> no cache-sa-maximum	配置缓存最大数目。 恢复默认缓存最大数目。

1.4.7 MSDP举例

案例 1: MSDP 功能。

组播配置:

1. 假设有组播服务器上提供组播地址 224.1.1.1 的节目, 组播源开始发送数据包;
2. 连接组播源的指定路由器 DR (Designated Router) 将组播源发出的数据封装在 Register 报文里, 发给本域内的 RP (RP1);
3. RP 将报文解封装, 沿域内的共享树向下转发给域内的所有成员, 域内成员可以选择是否切换到源树上;
4. 同时, 域内 RP 作为源端 RP, 将生成一个 SA (Source Active, 活动源) 消息, 发

送给 MSDP 对等体 (RP2)。

5. 如果 MSDP 对等体所在的域里有组成员 (RP3)，RP3 将 SA 消息中封装的组播数据沿共享树下发到组成员的同时，向组播源发送加入消息；即 RP 创建(S, G)表项，向源端 DR 逐跳发送(S, G)加入消息(Join Message)，从而跨越各 PIM-SM 域直接加入以该组播源为根的 SPT。

如果某个 MSDP 对等体所在的域 (RP2) 里没有组成员，则 RP2 不会创建(S, G)表项，也不加入以该组播源为根的 SPT。

6. 当逆向转发路径建立起来之后，组播源发出的数据将直接发送到 RP3 上，RP 向共享树转发数据。此时，连接组成员的最后一跳路由器可以自行选择是否切换到 SPT 上。

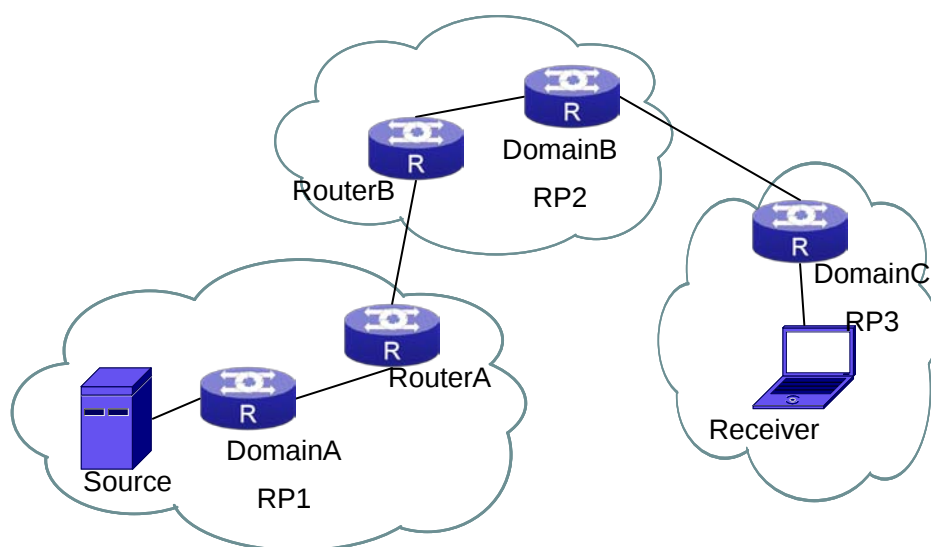


图 1-4 MSDP 对等体位置

配置步骤如下：

配置准备：

在每个路由器上启动单播路由协议和 PIM 协议，保证域内域间路由相通，域内组播正常。

假设 Domain A 中的组播服务器 S 上提供组播地址 224.1.1.1 的节目，Domain C 有主机 R 点播该节目，没有使能 MSDP 之前点播不到该节目，完成以下配置之后，R 能收看 S 的节目。

Domain A 的 RP1:

```
Switch#config
```

```
Switch(config)#interface vlan 1
```

```
Switch(Config-if-Vlan1)#ip address 10.1.1.1 255.255.255.0
```

```
Switch(Config-if-Vlan1)#exit
```

```
Switch(config)#router msdp
```

```
Switch(router-msdp)#peer 10.1.1.2
```

Domain A 的 Router A:

```
Switch#config
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ip address 20.1.1.2 255.255.255.0
Switch(Config-if-Vlan2)#exit
Switch(config)#router msdp
Switch(router-msdp)#peer 10.1.1.1
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 20.1.1.1
```

Domain B 的 Router B:

```
Switch#config
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ip address 20.1.1.1 255.255.255.0
Switch(Config-if-Vlan2)#exit
Switch(config)#interface vlan 3
Switch(Config-if-Vlan3)#ip address 30.1.1.1 255.255.255.0
Switch(Config-if-Vlan3)#exit
Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.2
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 30.1.1.2
```

Domain B 的 RP2:

```
Switch#config
Switch(config)#interface vlan 3
Switch(Config-if-Vlan3)#ip address 30.1.1.2 255.255.255.0
Switch(config)#interface vlan 4
Switch(Config-if-Vlan4)#ip address 40.1.1.2 255.255.255.0
Switch(Config-if-Vlan4)#exit
Switch(config)#router msdp
Switch(router-msdp)#peer 30.1.1.1
Switch(config)#router msdp
Switch(router-msdp)#peer 40.1.1.1
```

Domain C 的 RP3:

```
Switch(config)#interface vlan 4
Switch(Config-if-Vlan1)#ip address 40.1.1.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#router msdp
Switch(router-msdp)#peer 40.1.1.2
```

案例 2: MSDP Mesh-Group 应用。

Mesh-Group 规则可以在全连接组中有效的减少 SA 消息的泛洪。通常把同一个域中全连接的所有 Peer，配置为一个 Mesh-Group，且所有组成员均使用相同的组名称。

如图，对同域中四个全连接的 Peer 配置了 Mesh-Group 规则后，从 SA 消息的转发情况可看出，SA 消息的泛洪情况得到了很好的解决。

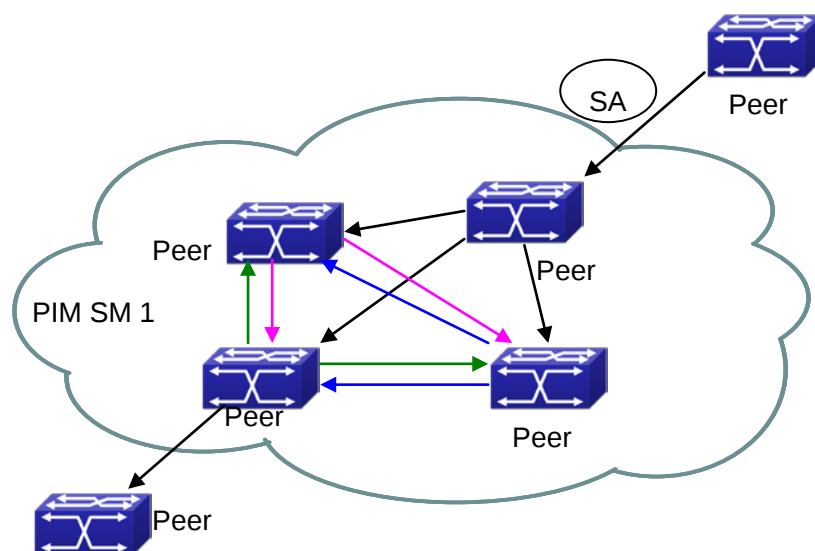


图 1-5 SA 消息泛洪

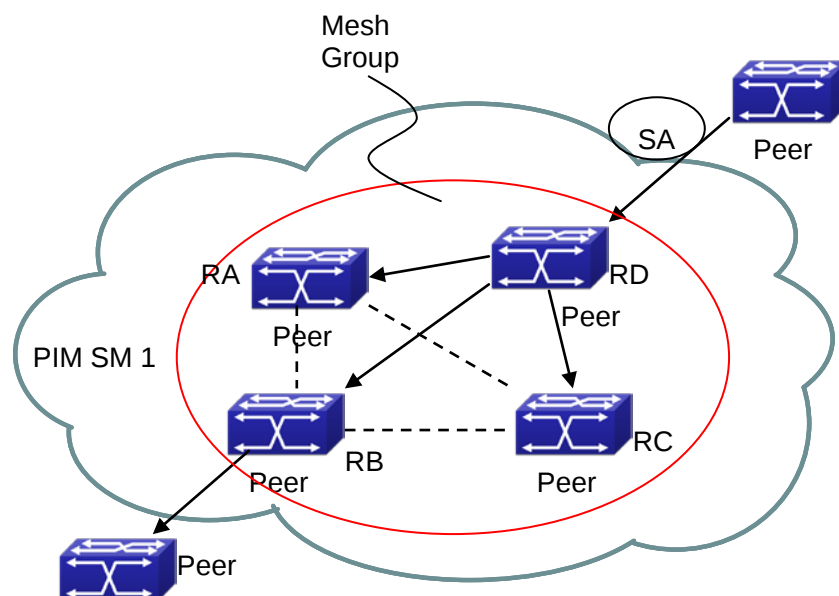


图 1-6 Mesh-Group 下控制 SA 消息泛洪

配置步骤如下：

Router A:

```
Switch#config
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ip address 20.1.1.1 255.255.255.0
Switch(Config-if-Vlan2)#exit
Switch(config)#interface vlan 3
Switch(Config-if-Vlan3)#ip address 30.1.1.1 255.255.255.0
Switch(Config-if-Vlan3)#exit
Switch(config)#router msdp
Switch(router-msdp)#peer 10.1.1.2
Switch(router-msdp)#mesh-group test-1
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 20.1.1.4
Switch(router-msdp)#mesh-group test-1
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 30.1.1.3
Switch(router-msdp)#mesh-group test-1
Switch(msdp-peer)#exit
```

Router B:

```
Switch#config
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#interface vlan 4
Switch(Config-if-Vlan4)#ip address 40.1.1.2 255.255.255.0
Switch(Config-if-Vlan4)#exit
Switch(config)#interface vlan 6
Switch(Config-if-Vlan6)#ip address 60.1.1.2 255.255.255.0
Switch(Config-if-Vlan6)#exit
Switch(config)#router msdp
Switch(router-msdp)#peer 10.1.1.1
Switch(router-msdp)#mesh-group test-1
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 40.1.1.4
Switch(router-msdp)#mesh-group test-1
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 60.1.1.3
Switch(router-msdp)#mesh-group test-1
```

Router C:

```
Switch#config
Switch(config)#interface vlan 4
Switch(Config-if-Vlan4)#ip address 40.1.1.4 255.255.255.0
Switch(Config-if-Vlan4)#exit
Switch(config)#interface vlan 5
Switch(Config-if-Vlan5)#ip address 50.1.1.4 255.255.255.0
Switch(Config-if-Vlan5)#exit
Switch(config)#interface vlan 6
Switch(Config-if-Vlan6)#ip address 60.1.1.4 255.255.255.0
Switch(Config-if-Vlan6)#exit
Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp)#mesh-group test-1
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 40.1.1.4
Switch(router-msdp)#mesh-group test-1
Switch(msdp-peer)#exit
```

```
Switch(router-msdp)#peer 60.1.1.2  
Switch(router-msdp)#mesh-group test-1
```

Router D:

```
Switch#config  
Switch(config)#interface vlan 2  
Switch(Config-if-Vlan2)#ip address 20.1.1.4 255.255.255.0  
Switch(Config-if-Vlan2)#exit  
Switch(config)#interface vlan 4  
Switch(Config-if-Vlan1)#ip address 40.1.1.4 255.255.255.0  
Switch(Config-if-Vlan1)#exit  
Switch(config)#interface vlan 5  
Switch(Config-if-Vlan5)#ip address 50.1.1.4 255.255.255.0  
Switch(Config-if-Vlan5)#exit  
Switch(config)#router msdp  
Switch(router-msdp)#peer 20.1.1.1  
Switch(router-msdp)#mesh-group test-1  
Switch(msdp-peer)#exit  
Switch(router-msdp)#peer 40.1.1.2  
Switch(router-msdp)#mesh-group test-1  
Switch(msdp-peer)#exit  
Switch(router-msdp)#peer 50.1.1.3  
Switch(router-msdp)#mesh-group test-1
```

1.4.8 MSDP排错帮助

在配置、使用 MSDP 功能时，可能会由于物理连接、配置错误等原因导致 MSDP 未能正常运行。因此，用户应注意以下要点：

- ☞ 应该保证物理连接的正确无误
- ☞ 保证各个 Peer 之间路由可达，即域内和域间网络层互通
- ☞ 保证各个域内的组播协议使用 PIM-SM，PIM-SM 配置正确并且运行正常
- ☞ 保证 MSDP 已经使能，配置的 Peer 使用的接口是 UP 的
- ☞ 使用 **show msdp gloabl** 命令查看 MSDP 配置信息是否正确

如果使用检查仍无法解决 MSDP 的问题，那么请使用 **debug msdp** 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给本公司技术服务中心。

1.5 ANYCAST RP配置

1.5.1 ANYCAST RP介绍

基于 PIM 协议的 Anycast RP 是一种为了让 RP 失效能够尽快恢复而提供冗余的技术，Anycast-RP 地址通常是配置在 loopback 接口上的地址。

Anycast RP 的核心思想是在整个网络上配置的 RP 地址，存在于多台组播路由器上(通常的情况是在各个提供 ANYCAST RP 的设备上都使用 LOOPBACK 接口，并配置 RP 地址在这个接口上，使用最长的掩码)，而单播路由算法将决定了 PIM 路由器总是能找到离自己最近的 RP，因此对于比较大的网络提供了更短更快的找到 RP 的路径。而一旦正在使用的某一个 RP 失效，单播路由算法将保证 PIM 路由器很快找到新的 RP 路径，从而使组播服务迅速恢复。多个 RP 会出现新的问题，即如果组播源和接收者注册到不同的 RP，会导致有的接收者不能接收到组播源数据（注册报文显然只会青睐离自己的最近的 RP）。因此，为了在各 RP 间保持联络，Anycast RP 规定离组播源最近的 RP 在收到注册报文时应将源注册信息转发通知给其他 RP，保证所有 RP 上的加入者都可以找到该组播源。

基于 PIM 协议的 Anycast RP 具体实现方法是：在每个配置了 Anycast RP 的交换机上维护一份 ANYCAST RP 的列表，并使用另一个地址作为他们之间互相识别的标志，在一台 Anycast RP 设备收到注册消息后，以标志自己的地址作为源地址向其它 Anycast RP 设备发送注册消息，以达到让其它设备也知道本源的目的。

1.5.2 ANYCAST RP配置任务

- 1.启动 ANYCAST RP v4 功能
- 2.配置 ANYCAST RP v4

1.启动 ANYCAST RP v4 功能

命令	解释
全局配置模式	
ip pim anycast-rp	启动 ANYCAST RP 功能。（必须）
no ip pim anycast-rp	no 操作关闭全局 ANYCAST RP 功能。

2.配置 ANYCAST RP v4

(1) 配置候选 RP

命令	解释
全局配置模式	
ip pim rp-candidate {vlan<vlan-id> loopback<index> <ifname>} [<A.B.C.D>] [<priority>]	目前 PIM-SM 已允许配置 Loopback 接口作为候选 RP。（必须） 需要注意，ANYCAST RP 协议可以配置

no ip pim rp-candidate	Loopback 接口或普通三层 VLAN 接口作为候选 RP。为使网络中 PIM 路由器找到 RP 位置，应将候选 RP 接口添加到路由中。 no 操作取消本路由器候选 RP 配置。
-------------------------------	---

(2) 配置 self-rp-address (本 RP 通信地址)

命令	解释
全局配置模式	
ip pim anycast-rp self-rp-address A.B.C.D no ip pim anycast-rp self-rp-address	在本路由器（作为 RP）上配置本路由器的 self-rp-address。该地址唯一标志本路由器，用于与其他 RPs 之间的通讯。 self-rp-address 具体作用有两个方面： 1 当本路由器（作为 RP）收到从 DR 单播过来的注册报文，需要将该注册报文向网络中其他 RP 转发，使得网络中所有 RP 获得源（S,G）状态。转发时，本路由器修改注册报文源地址为 self-rp-address。 2 当本路由器（作为 RP）收到从其他 RP 单播转发过来的注册报文，如注册报文目的地址为本路由器 self-rp-address，则建立（S,G）状态并反方向发送注册中止报文，注册中止报文目的地址即注册报文的源地址。 注意：self-rp-address 应为本路由器上某个三层接口地址，但在配置时我们允许此接口当前不存在。self-rp-address 是唯一的。 no 操作取消本路由器（作为 RP）用于与其他 RP 通信的 self-rp-address。

(3) 配置 other-rp-address (其他 RP 通信地址)

命令	解释
全局配置模式	
ip pim anycast-rp <anycast-rp-addr> <other-rp-addr> no ip pim anycast-rp <anycast-rp-addr> <other-rp-addr>	在本路由器（作为 RP）上配置 anycast-rp-addr 地址。该单播地址实际上就是在网络中多个 RP 上配置的 RP 地址，对应候选 RP 接口(或者 Loopback 接口)的地址。 anycast-rp-addr 具体作用有： 1 允许配置多个 anycast-rp-addr 地址，只有

	与当前配置的候选 RP 接口地址相同的 anycast-rp-addr 地址生效。此时对应该 anycast-rp-addr 地址的 other-rp-address 也才会生效。 2 配置时我们允许 anycast-rp-addr 对应的接口当前不存在。 在本路由器（作为 RP）上配置与本路由器通讯的其他 RP 的 other-rp-address。该单播地址标志其他 RP，用于与本地路由器之间的通讯。 other-rp-address 具体作用有两个方面： 1 当本路由器（作为 RP）收到从 DR 单播过来的注册报文，需要将该注册报文向网络中其他 RP 转发，使得网络中所有 RP 获得源（S，G）状态。转发时，本路由器修改注册报文目的地址为 other-rp-address。 2 对应一个 anycast-rp-addr 可以配置多个 other-rp-address，当收到 DR 单播过来的注册报文，依次向这些其他 RP 转发。 no 操作取消与本路由器通信的某个 other-rp-address。
--	---

1.5.3 ANYCAST RP典型案例

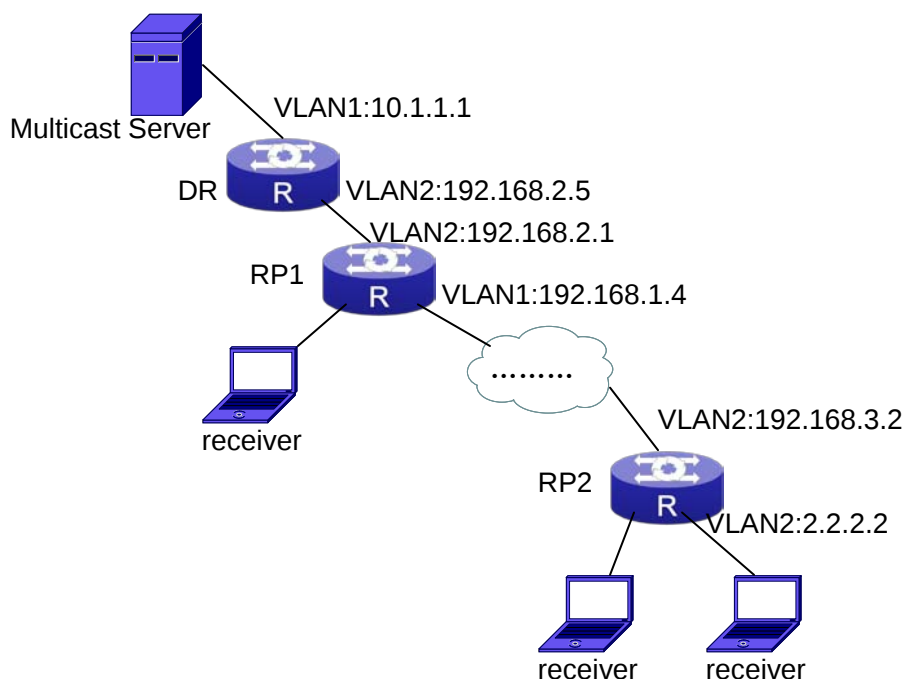


图 1-7 路由器 ANYCAST RP v4 功能

如图所示，整体网络环境为 PIM-SM，网络中提供了两台支持 ANYCAST RP 的路由器 RP1，RP2。组播源服务器发出的组播数据到达 DR 后，DR 依据单播路由算法向距离自己最近的 RP 单播发送组播源注册报文，此处为 RP1。在 RP1 收到来自 DR 的注册报文后，除了根据已加入自己的点播者向共享树下发，RP1 会在收到注册报文后将组播源注册信息转发通知给 RP2，保证所有 RP2 上的加入者都可以找到该组播源。由于在配置了 ANYCAST RP 的路由器 RP1 上维护了一份 ANYCAST RP 的列表，该列表保存了网络中所有其他 RP 的单播通讯地址，因此 RP1 收到注册消息后，以标志自己的 self-rp-address 地址作为源地地址向 RP2 转发注册消息。本图中云层代表处于 RP1 和 RP2 之间运行 PIM-SM 的网络。

配置步骤如下：

RP1 配置：

```
Switch#config
Switch(config)#interface loopback 1
Switch(Config-if-Loopback1)#ip address 1.1.1.1 255.255.255.255
Switch(Config-if-Loopback1)#exit
Switch(config)#ip pim rp-candidate loopback1
Switch(config)#ip pim bsr-candidate vlan 1
Switch(config)#ip pim multicast-routing
Switch(config)#ip pim anycast-rp
Switch(config)#ip pim anycast-rp self-rp-address 192.168.2.1
Switch(config)#ip pim anycast-rp 1.1.1.1 192.168.3.2
```

RP2 配置:

```
Switch#config
Switch(config)#interface loopback 1
Switch(Config-if-Loopback1)#ip address 1.1.1.1 255.255.255.255
Switch(Config-if-Loopback1)#exit
Switch(config)#ip pim rp-candidate loopback1
Switch(config)#ip pim multicast-routing
Switch(config)#ip pim anycast-rp
Switch(config)#ip pim anycast-rp self-rp-address 192.168.3.2
Switch(config)#ip pim anycast-rp 1.1.1.1 192.168.2.1
```

1.5.4 ANYCAST RP排错帮助

在配置、使用 ANYCAST RP 功能时，可能会由于物理连接、配置错误等原因导致 ANYCAST RP 未能正常运行。因此，用户应注意以下要点：

- ☞ 应该保证物理连接的正确无误
- ☞ 保证 PIM-SM 协议正确运行
- ☞ 保证全局配置模式下 ANYCAST RP 打开
- ☞ 保证全局配置模式下 self-rp-address 配置正确
- ☞ 保证全局配置模式下 other-rp-address 配置正确
- ☞ 保证各接口路由正确添加，包括作为 RP 的 loopback 接口也要正确加入路由
- ☞ 使用 show ip pim anycast rp status 命令查看 ANYCAST RP 配置信息是否正确

如果使用检查仍无法解决 ANYCAST RP 的问题，那么请使用 debug pim anycast-rp 调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给本公司技术服务中心。

1.6 PIM-SSM

1.6.1 PIM-SSM 介绍

源指定组播(PIM-SSM)是一种区别于传统组播的新的业务模式，它使用组播组地址和组播源地址来同时标志一个组播会话。SSM保留了传统PIM-SM模式中的主机显示加入组播组的高效性，但是跳过了PIM-SM模式中的共享树和RP规程。SSM直接建立由(S,G)标志的spt树，其中G表示组播组的地址，S表示发向组播组G的特定组播源的地址。SSM的一个(S,G)对也被称为一个频道。SSM特别适用于点到多点的组播服务，如网络体育频道，网络新闻频道等业务。在缺省情况下，SSM组播组地址范围限制在IP地址范围：

232.0.0.0-232.255.255.255内，但是可以根据需要对地址进行扩展。

PIM-DM的环境中 also 支持PIM-SSM。

1.6.2 PIM-SSM 配置任务序列

命令	解释
全局配置模式	
ip multicast ssm {default range <access-list-number >} no ip multicast ssm	该命令配置 pim ssm 组播组地址范围；本命令的 no 操作删除配置的 pim ssm 组播组。

1.6.3 PIM-SSM 典型案例

如下图所示，将switchA，switchB，switchC，switchD的以太网接口加入到相应VLAN中，并在各VLAN接口上启动PIM-SM协议，或者PIM-DM协议，全局启动PIM-SSM。本例以PIM-SM协议为例。

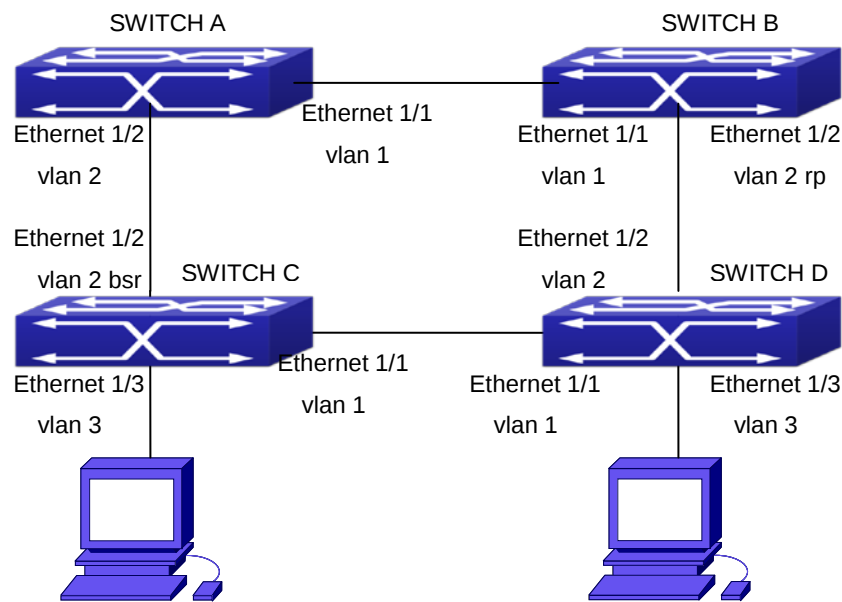


图 1-8 PIM-SSM 典型环境

switchA 和 switchB，switchC，switchD 配置步骤如下：

(1) 配置 switchA：

```
switch(config)#ip pim multicast-routing
switch(config)#interface vlan 1
switch(Config-If-Vlan1)#ip pim sparse-mode
switch(Config-If-Vlan1)#exit
switch(config)#interface vlan 2
switch(Config-If-Vlan2)#ip pim sparse-mode
```

```
switch(Config-If-Vlan2)#exit
switch(config)#access-list 1 permit 224.1.1.1 0.0.0.255
switch(config)#ip multicast ssm range 1
```

(2) 配置 switchB:

```
switch(config)#ip pim multicast-routing
switch(config)#interface vlan 1
switch(Config-If-Vlan1)#ip pim sparse-mode
switch(Config-If-Vlan1)#exit
switch(config)#interface vlan 2
switch(Config-If-Vlan2)#ip pim sparse-mode
switch(Config-If-Vlan2)#exit
switch(config)# ip pim rp-candidate vlan2
switch(config)#access-list 1 permit 224.1.1.1 0.0.0.255
switch(config)#ip multicast ssm range 1
```

(3) 配置 switchC:

```
switch(config)#ip pim multicast-routing
switch(config)#interface vlan 1
switch(Config-If-Vlan1)#ip pim sparse-mode
switch(Config-If-Vlan1)#exit
switch(config)#interface vlan 2
switch(Config-If-Vlan2)#ip pim sparse-mode
switch(Config-If-Vlan2)#exit
switch(config)#interface vlan 3
switch(Config-If-Vlan3)#ip pim sparse-mode
switch(Config-If-Vlan3)# exit
switch(config)#ip pim bsr-candidate vlan2 30 10
switch(config)#access-list 1 permit 224.1.1.1 0.0.0.255
switch(config)#ip multicast ssm range 1
```

(4) 配置 switchD:

```
switch(config)#ip pim multicast-routing
switch(config)#interface vlan 1
switch(Config-If-Vlan1)#ip pim sparse-mode
switch(Config-If-Vlan1)#exit
switch(config)#interface vlan 2
switch(Config-If-Vlan2)#ip pim sparse-mode
switch(Config-If-Vlan2)#exit
switch(config)#interface vlan 3
switch(Config-If-Vlan3)#ip pim sparse-mode
```

```
switch(Config-If-Vlan3)#exit
switch(config)#access-list 1 permit 224.1.1.1 0.0.0.255
switch(config)#ip multicast ssm range 1
```

1.6.4 PIM-SSM 排错帮助

在配置、使用 PIM-SSM 协议时，可能会由于物理连接、配置错误等原因导致 PIM-SSM 协议未能正常运行。因此，用户应注意以下要点：

- ☞ 应该保证物理连接的正确无误；
- ☞ 保证接口和链路协议是 UP（使用 show interface 命令）；
- ☞ 保证全局配置模式下 PIM 协议打开（使用 ip pim multicast-routing）；
- ☞ 保证接口上配置 PIM-SM（使用 ip pim sparse-mode）；
- ☞ 保证全局模式下配置 SSM；
- ☞ 组播协议需使用单播路由进行 RPF 检查，因此必须首先确保单播路由的正确性。

如果使用检查仍无法解决问题，那么请使用 debug pim event/debug pim packet 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给本公司技术服务中心。

1.7 DVMRP

1.7.1 DVMRP 介绍

DVMRP（Distance Vector Multicast Routing Protocol）协议即“距离向量组播路由协议”。它是一种密集模式的组播路由协议，采用类似 RIP 方式的路由交换给每个源建立了一个转发广播树，然后通过动态的剪枝/嫁接给每个源建立起一个截断广播树，也就是到源的最短路径树。通过反向路径检查(RPF)来决定组播包是否应该被转发到下游。

DVMRP 的一些重要特性是：

1. 用于决定反向路径检查信息的路由交换以距离向量为基础（方式与 RIP 相似）
2. 路由交换更新周期性的发生（缺省为 60 秒）
3. TTL 上限=32 跳（而 RIP 是 16）
4. 路由更新包括掩码，支持 CIDR

相对单播路由来说，组播路由是一种颠倒的路由（也就是，你所感兴趣的是信息包从哪里来而不是到哪里去），因此在 DVMRP 路由表中的信息是被用于确定是否在正确的接口收到一个输入的组播信息包。否则，为了防止组播循环将放弃该信息包。

把为了确定信息包到达正确的接口所进行的测试称为 RPF 检查。当有组播数据包到达某个接口，通过查找 DVMRP 路由表来决定到源网络的反向路径。如果数据包到达的接口是用于向源传送单播信息的接口，则逆向路径检查正确，数据包从所有下游接口转发出去。如果不是，则可能是出现了故障，丢弃该组播包。

因为不是所有的交换机都支持组播，DVMRP 支持隧道组播通信，隧道是在被不支持组播路由的交换机隔开的 DVMRP 交换机之间发送组播数据报的一种方法。它充当两个

DVMRP交换机之间的虚拟网络。组播数据包被封装在单播数据包之内，直接发送到下一个支持组播的交换机。DVMRP协议平等对待隧道接口与一般的物理接口。

如果在一个多入口网络上连接了两个或两个以上的交换机，就可能会把一个数据包的多份拷贝发送到该子网上。因此必须指定一个指定的转发者，DVMRP在利用路由交换的机制来达到这一目的，当多入口网络上的两个交换机交换路由信息时，就会互相知道对方到源网络的路由度量，因此到源网络的度量最小的交换机成为该子网上的指定转发者，如果度量一致，则IP地址较低的获胜。

当交换机的某个接口配置了运行DVMRP协议以后，就在该接口上向其他的DVMRP交换机组播探寻（Probe）消息，用于发现邻居且互相探知对方的能力（Capabilities）。如果在邻居超时前一直没有收到该邻居的Probe消息，则认为该邻居丢失。

在DVMRP中，源网络路由选择信息用和RIP相同的基本方式交换。也就是说，路由报告消息定期（缺省为60秒）在DVMRP邻居之间发送。DVMRP路由选择表中的路由信息被用于建立源分布树，也就是决定通过哪一个邻居能够到达发送组播信息的源，到该邻居的接口被称为上游接口。路由报告包含源网络（用掩码）地址和用于路由尺度的跳数项。

为了转发能够正确的完成，每个DVMRP交换机都需要知道哪些下游交换机需要通过它从某个特定的源网络接收组播信息。当接收到某个特定的源发来的包后，DVMRP交换机首先从所有的下游接口，也就是在该接口上有其他的对该特定源表示了依赖性的DVMRP交换机，把该组播包广播出去。当接口上收到了某个下游交换机发送的剪枝（Prune）消息后，就把该交换机剪枝。DVMRP交换机使用毒性反转来通知某个特定源的上游交换机：“我是你的下游”。DVMRP交换机通过把它广播的某个特定源的路由度量加上无限（32）来回应到该源上游交换机来完成毒性反转。这意味着度量正确值为1到2*无限（32）-1或1到63，1到31意味着可以到达源网络，32意味着源网络不可达，33到63意味着产生该报告（Report）消息的交换机依赖上游路由器来接收特定源的组播信息。

1.7.2 配置任务序列

- 1、全局启动和关闭 DVMRP（必须）
- 2、配置在接口启动和关闭 DVMRP 协议（必须）
- 3、配置 DVMRP 辅助参数（可选）
 - 配置 DVMRP 接口参数
 - 1) 配置 DVMRP 接口上发送 report 报文的延迟和每次发送的报文数
 - 2) 配置 DVMRP 接口 metric 值
 - 3) 配置 DVMRP 是否与不能 Prune/Graft 的 DVMRP 路由器建立邻居
- 4、配置 DVMRP 隧道

1. 全局启动 DVMRP 协议

在三层交换机上运行 DVMRP 路由协议的基本配置很简单，首先需在全局模式下打开 DVMRP 开关。

命令	解释
----	----

全局配置模式	
[no] ip dvmrp multicast-routing	全局启动 DVMRP 协议, 本命令的 no 操作全局关闭 DVMRP 协议。(必须)

2. 在接口上启动 DVMRP 协议

在三层交换机上运行 DVMRP 路由协议的基本配置很简单, 在全局启动 DVMRP 协议后, 需在相应的接口下打开 DVMRP 开关。

命令	解释
接口配置模式	
ip dvmrp enable no ip dvmrp	在接口上启动 DVMRP 协议, 本命令的 no 操作在接口上关闭 DVMRP 协议。

3. 配置 DVMRP 辅助参数

(1) 配置 DVMRP 接口参数

- 1) 配置 DVMRP 接口上发送 report 报文的延迟和每次发送的报文数
- 2) 配置 DVMRP 接口 metric 值
- 3) 配置 DVMRP 是否与不能 Prune/Graft 的 DVMRP 路由器建立邻居

命令	解释
接口配置模式	
ip dvmrp output-report-delay <delay_val> [<burst_size>] no ip dvmrp output-report-delay	配置接口上发送 DVMRP report 报文的延时以及每次发送所发送的报文数量, 本命令的 no 操作恢复默认值。
ip dvmrp metric <metric_val> no ip dvmrp metric	配置接口 DVMRP report 报文度量值; 本命令的 no 操作恢复为缺省值。
ip dvmrp reject-non-pruners no ip dvmrp reject-non-pruners	配置接口上拒绝与 non pruning/grafting 的 DVMRP 路由器建立邻居关系, 本命令的 no 操作恢复为可以建立邻居关系。

4. 配置 DVMRP 隧道

命令	解释
接口配置模式	
ip dvmrp tunnel <index> <src-ip> <dst-ip> no ip dvmrp tunnel {<index> <src-ip> <dst-ip>}	本命令配置一条 DVMRP 隧道; 本命令的 no 操作删除一条 DVMRP 隧道。

1.7.3 DVMRP 典型案例

如下图，将switchA 和switchB 的以太网接口加入到相应的VLAN中，并在各VLAN接口上启动DVMRP。

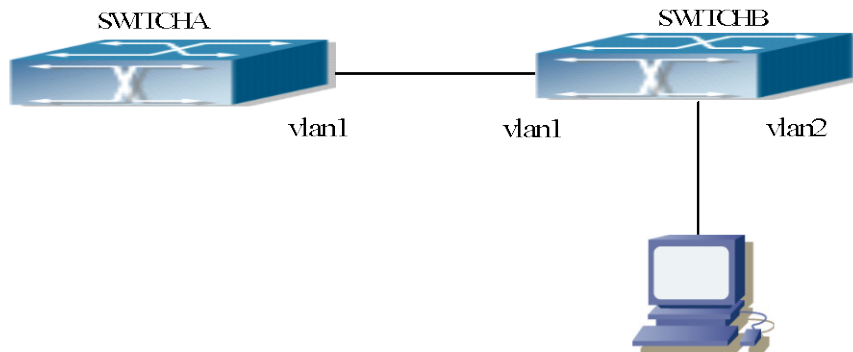


图 1-9 DVMRP 网络拓扑示意图

switchA 和switchB配置步骤如下：

(1) 配置SwitchA:

```
Switch (config)#ip dvmrp multicast-routing
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)# ip address 10.1.1.1 255.255.255.0
Switch(Config-if-Vlan1)# ip dvmrp enable
```

(2) 配置SwitchB:

```
Switch (config)#ip dvmrp multicast-routing
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)# ip address 10.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)# ip dvmrp enable
Switch(Config-if-Vlan1)#exit
Switch (config)#interface vlan 2
Switch(Config-if-Vlan2)# ip address 20.1.1.1 255.255.255.0
Switch(Config-if-Vlan2)# ip dvmrp enable
```

由于 DVMRP 自己不依赖单播路由协议，因此无需配置单播路由协议，这是与 PIM-DM 和 PIM-SM 所不同的。

1.7.4 DVMRP排错帮助

在配置、使用 DVMRP 协议时，可能会由于物理连接、配置错误等原因导致 DVMRP 协议未能正常运行。因此，用户应注意以下要点：

- ☞ 首先应该保证物理连接的正确无误；
- ☞ 其次，保证接口和链路协议是 UP（使用 show interface 命令）；
- ☞ 请检查接口是否已配置了正确的 IP 地址；

- ☞ 然后，在接口上启动 DVMRP 协议（使用 `ip dvmrp enable` 和 `ip dvmrp multicast-routing` 命令）；
- ☞ 组播协议需使用单播路由进行 RPF 检查，因此必须首先确保单播路由的正确性（DVMRP 使用自己的单播路由表，查看请使用 `show ip dvmrp route` 命令）。

如果仍无法解决 DVMRP 的问题，那么请使用 `debug dvmrp` 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给本公司技术服务中心。

1.8 DCSCM

1.8.1 DCSCM介绍

DCSCM（Destination Control and Source Control Multicast）技术主要包含三个方面，即组播信源可控、组播用户可控及面向服务优先级的策略组播。

受控组播技术的组播信源可控技术主要采取以下的方式进行：

1. 在边缘交换机上，如果配置的源受控组播，只有指定源发出的指定组的组播数据才能通过。
2. 对于处于 PIM-SM 核心地位的 RP 交换机，对于指定源及指定组以外的 REGISTER 信息，直接发送 REGISTER_STOP，而不允许建立表项。（该任务在 PIM-SM 模块中实现）。

受控组播技术的组播用户可控技术的实现基于对用户发出的 IGMP REPORT 报文的控制，因此进行控制的模块是 IGMP Snooping 和 IGMP 模块，其控制逻辑包括以下三种，即根据发送报文的 VLAN+MAC 地址进行控制，根据发送报文的 IP 地址进行控制和根据报文进入的端口进行控制。其中 IGMP Snooping 可以同时使用上述三种方式进行控制，而 IGMP 模块由于处于三层，仅针对发送报文的 IP 地址进行控制。

受控组播技术的面向服务优先级的策略组播采用下述的方式：对于限定范围的组播数据，在接入端就设置用户指定的优先级，使得数据在干道端口（TRUNK）上以更高的优先级发送，从而在整个网络上保证其以用户指定的优先级传送。

1.8.2 DCSCM配置任务序列

1. 源受控的配置
2. 目的受控的配置
3. 组播策略的配置

1. 源受控的配置

源受控的配置分三个部分，首先是全局启动源受控，全局启动源受控的命令如下：

命令	解释
全局配置模式	

ip multicast source-control(必须) no ip multicast source-control	全局启动源控制，本命令的 no 操作全局关闭源控制。值得注意的是，全局启动源控制后，所有组播报文都默认丢弃。所有源控制配置都要在全局启动后才可以进行，而只有关闭所有已经配置的规则后，才可以全局关闭源控制。
---	--

其次是配置源控制的规则，它使用与 ACL 相同的方式配置，使用 5000—5099 的 ACL 号，每个规则号最多可配置 10 个规则，值得注意的是，这些规则是有顺序的，先配置的在最前面，一旦所配置的规则得到匹配，其后面的规则将不会起作用，所以全局允许的规则一定要配置在最后。其命令如下

命令	解释
全局配置模式	
access-list <5000-5099> {deny permit} ip {{<source> <source-wildcard>}}{<host-source <source-host-ip>}}any-source} {{<destination> <destination-wildcard>}}{<host-de stination <destination-host-ip>}}any-destin ation} no access-list <5000-5099> {deny permit} ip {{<source> <source-wildcard>}}{<host-source <source-host-ip>}}any-source} {{<destination> <destination-wildcard>}}{<host-de stination <destination-host-ip>}}any-destin ation}	用于配置源受控使用的规则，该规则只有应用到指定的端口上时才可以生效。使用其 NO 形式可以删除指定的规则。

最后是把配置的规则配置到指定的端口上。
注意：由于配置的规则要占据硬件的表项，配置过多的规则可能导致由于底层表项满而配置失败，因此建议用户尽可能使用简单的规则。配置命令如下

命令	解释
端口配置模式	
ip multicast source-control access-group <5000-5099> no ip multicast source-control access-group <5000-5099>	用于把源受控使用的规则配置到端口上，其 NO 形式取消该配置。

2. 目的受控的配置

目的受控的配置与源受控配置相似，也是分三个步骤。

首先要全局打开目的受控，由于目的受控要防止未获授权的用户接收到组播数据，因此配置全局目的受控后，交换机对收到的组播数据不再广播，因此，应当避免在启动了目的受控的交换机上同一 VLAN 内连接两台或以上的其它三层交换机。其配置命令如下

命令	解释
全局配置模式	
multicast destination-control(必须) no multicast destination-control	全局同时启动 IPv4 和 IPv6 目的受控组播,本命令的 no 操作全局关闭目的控制。所有其它的配置都只有在全局启动后才能生效。

其次是配置组播目的受控 profile 规则列表，使用 1—50 的 profile-id 号。

命令	解释
全局配置模式	
profile-id <1-50> {deny permit} {{<source/M> }}{host-source <source-host-ip> (range <2-65535>)}}any-source} {{<destination/M> }}{host-destination <destination-host-ip> (range <2-255>)}}any-destination} no profile-id <1-50>	配置目的受控的 profile 规则。其 no 操作用于删除该 profile 规则。

最后是配置目的控制规则，它与源控制相似，只是使用 6000—7999 的 ACL 号。

命令	解释
全局配置模式	

<pre> access-list <6000-7999> {{{add delete} profile-id WORD} {{deny permit} (ip) {{<source/M> }}{host-source <source-host-ip> (range <2-65535>)}}any-source} {{<destination/M>}}{{host-destination <destination-host-ip> (range <2-255>)}}any-destination}} no access-list <6000-7999> {deny permit} ip {{<source> <source-wildcard>}}{{host-source <source-host-ip> {range <2-65535>)}}any-source} {{<destination> <destination-wildcard>}}{{host-destination <destination-host-ip> {range <2-255>)}}any-destination} </pre>	用于配置目的受控使用的规则，该规则只有应用到指定的源 IP 或 VLAN-MAC、端口上时才可以生效。使用其 NO 形式可以删除指定的规则。
--	---

最后要把该规则配置到指定的源 IP、源 VLAN MAC 或指定端口上。这里需要注意的是，由于上面所说的情况，只有在启动 IGMP-SNOOPING 的情况下才可以全面使用这些规则，而如果没有启动 IGMP-SNOOPING，则只有源 IP 的规则才能在 IGMP 协议使用。其配置命令如下：

命令	解释
端口配置模式	
<pre> ip multicast destination-control access-group <6000-7999> no ip multicast destination-control access-group <6000-7999> </pre>	用于把目的受控使用的规则配置到端口上，其 NO 形式取消该配置。
全局配置模式	
<pre> ip multicast destination-control <1-4094> <macaddr> access-group <6000-7999> no ip multicast destination-control <1-4094> <macaddr> access-group <6000-7999> </pre>	用于把目的受控使用的规则配置到指定的 VLAN-MAC 上，其 NO 形式取消该配置。
<pre> ip multicast destination-control <IPADDRESS/M> access-group <6000-7999> no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999> </pre>	用于把目的受控使用的规则配置到指定的源 IP 地址/掩码上，其 NO 形式取消该配置。

3. 组播策略的配置

组播策略使用为指定的组播数据指定优先级的方式达到保证特定用户需求的效果，值得注意的是组播数据只有在干道端口上传输才能保证数据一直得到重点照顾。其配置很简单，只有一个命令，即为指定的组播设定优先级，命令如下：

命令	解释
全局配置模式	
[no] ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority>	配置组播策略，为特定范围的源、组指定优先级，范围为<0-7>。

1.8.3 DCSCM典型案例

1. 源受控

为了防止一台边缘交换机随意发布组播数据，我们在边缘交换机上配置，只有在端口 Ethernet1/5 的交换机才允许发送组播数据，且数据的组必须是 225.1.2.3。而上连端口 Ethernet1/10 可以不受限制的转发组播数据，则我们可以进行如下配置。

```
Switch (config)#access-list 5000 permit ip any host 225.1.2.3
```

```
Switch (config)#access-list 5001 permit ip any any
```

```
Switch (config)#ip multicast source-control
```

```
Switch (config)#interface ethernet1/5
```

```
Switch (Config-If-Ethernet1/5)#ip multicast source-control access-group 5000
```

```
Switch (config)#interface ethernet1/10
```

```
Switch (Config-If-Ethernet1/10)#ip multicast source-control access-group 5001
```

2. 目的受控

我们要限制地址在 10.0.0.0/8 网段的用户不能加入 238.0.0.0/8 的组，我们可以做如下配置：

首先在其所在的 VLAN(这里认为是 VLAN2)内要启动 IGMP Snooping。

```
Switch (config)#ip igmp snooping
```

```
Switch (config)#ip igmp snooping vlan 2
```

然后配置相关的目的控制访问列表，并配置指定的 IP 地址使用该访问列表。

```
Switch (config)#access-list 6000 deny ip any 238.0.0.0 0.255.255.255
```

```
Switch (config)#access-list 6000 permit ip any any
```

```
Switch (config)#multicast destination-control
```

```
Switch (config)#ip multicast destination-control 10.0.0.0/8 access-group 6000
```

这样，该网段的用户就只能加入 238.0.0.0/8 以外的组了。

或者可以按照下面添加 profile 列表的方式进行配置相关的目的控制访问列表。

```
Switch (config)#profile-id 1 deny ip any 238.0.0.0 0.255.255.255
```

```
Switch (config)#access-list 6000 add profile-id 1
```

```
Switch (config)#multicast destination-control
```

```
Switch (config)#ip multicast destination-control 10.0.0.0/8 access-group 6000
```

3. 组播策略

服务器 210.1.1.1 正在组 239.1.2.3 上发布重要的组播数据，我们可在其接入交换机上配置如下：

```
Switch(config)#ip multicast policy 210.1.1.1/32 239.1.2.3/32 cos 4
```

这样该组播流在通过本交换机的 TRUNK 端口通向其它交换机时，将拥有值为 4 的优先级（通常这已经比较高了，更高的可能是协议数据了，若设置更高的优先级，在该组播数据太多时，有可能造成交换机协议行为的不正常）。

1.8.4 DCSCM排错帮助

DCSCM 模块本身作用与 ACL 相似，发生问题通常与不当的配置有关，请您详细阅读上面的说明，如果仍不能确定问题发生的原因，请把您的配置和希望达到的效果发送给本公司的售后服务人员。

1.9 IGMP

1.9.1 IGMP介绍

IGMP（Internet Group Management Protocol，因特网组管理协议）是TCP/IP协议族中负责IP 组播成员管理的协议。它用来在IP 主机和与其直接相邻的组播交换机之间建立、维护组播组成员关系。IGMP 不包括组播交换机之间的组成员关系信息的传播与维护，这部分工作由各组播路由协议完成。所有参与组播的主机必须实现IGMP 协议。

参与IP 组播的主机可以在任意位置、任意时间、成员总数不受限制地加入或退出组播组。组播交换机不需要也不可能保存所有主机的成员关系，它只是通过IGMP 协议了解每个接口连接的网段上是否存在某个组播组的接收者，即组成员。而主机方只需要保存自己加入了哪些组播组。

IGMP 在主机与路由器之间是不对称的：主机需要响应组播交换机的IGMP查询报文，即以成员资格报告报文响应；交换机周期性发送成员资格查询报文，然后根据收到的响应报文确定某个特定组在自己所在子网上是否有主机加入，并且当收到主机的退出组的报告时，发出特定组的查询（IGMP 版本2），以确定某个特定组是否已无成员存在。

到目前为止，IGMP 有三个版本：IGMP 版本1（由RFC1112 定义）、IGMP版本2（由RFC2236 定义）和IGMP 版本3（RFC3376定义）。

IGMP 版本2 对版本1 所做的改进主要有：

1. 共享网段上组播交换机的选举机制

共享网段即一个网段上有多个组播交换机的情况。在这种情况下，由于此网段下运行IGMP 的交换机都能从主机那里收到成员资格报告消息，因此，只需要一个交换机发送成员资格查询消息，这就需要一个交换机选举机制来确定一个交换机作为查询器。在IGMP 版本1 中，查询器的选择由组播路由协议决定；IGMP 版本2 对此做了改进，规定同一网段

上有多个组播交换机时，具有最低IP 地址的组播交换机被选举出来充当查询器。

2. IGMP 版本2 增加了离开组机制

在IGMP 版本1 中，主机悄然离开组播组，不会给任何组播交换机发出任何通知。造成组播交换机只能依靠组播组响应超时来确定组播成员的离开。而在版本2 中，当一个主机决定离开一个组播组时，如果它是对最近一条成员资格查询消息作出响应的主机，那么它就会发送一条离开组的消息。

3. IGMP 版本2 增加了对特定组的查询

在IGMP 版本1 中，组播交换机的一次查询，是针对该网段下的所有组播组。这种查询称为普通组查询。在IGMP 版本2 中，在普通组查询之外增加了特定组的查询，这种查询报文的目的IP 地址为该组播组的IP 地址，报文中的组地址域部分也为该组播组的IP 地址。这样就避免了属于其它组播组成员的主机发送响应报文。

4. IGMP 版本2 增加了最大响应时间字段

IGMP 版本2 增加最大响应时间字段，以动态地调整主机对组查询报文的响应时间。

版本3主要特点是允许主机选择接收或者拒绝特定的源，是SSM（Source-Specific Multicast）组播的基础。例如：当一个主机对于某个组G发出INCLUDE{10.1.1.1, 10.1.1.2}的报告时，意味着主机需要路由器转发组G中来自10.1.1.1和10.1.1.2的流量；当一个主机对组G发出EXCLUDE{192.168.1.1}的报告时，意味着主机需要组G的所有源发来的流量，除了192.168.1.1。这就和之前的IGMP有了很大的区别。

IGMP 版本3对IGMP 版本2所作的改进主要有：

1. 维护的状态为组和源列表，不仅仅是 IGMPv2 中的组。
2. 在 IGMPv3 状态中定义了与 IGMPv1 和 IGMPv2 的互操作。
3. IP 服务接口改变，从而允许特定的源列表。
4. 查询者在查询分组中包含其 Robustness Variable 和 Query Interval 以允许与非查询者的这些变量同步。
5. 查询消息中的 Max Response Time 有一个指数级的范围，最大值从 v2 的 25.5 秒增加到约 53 分钟，可用于有海量系统的链路。
6. 为增强健壮性，主机重传 State-Change 消息。
7. 定义了附加数据以适应将来的扩展。
8. 报告分组被发送到 224.0.0.22，用于协助二层交换机的 IGMP Snooping。
9. 报告分组可以包含多个组记录，允许使用少量分组报告完整的当前状态。
10. 主机不再进行抑止操作，简化了实现并且允许直接的成员资格跟踪。
11. 在查询消息中新的路由器方抑止处理（S 标志）修改了 IGMPv2 存在的健壮性问题。

1.9.2 配置任务序列

- 1、启动 IGMP（必须）
- 2、配置 IGMP 辅助参数（可选）

（1）配置 IGMP 组 group 参数

- 1) 配置 IGMP 组过滤条件
- 2) 配置 IGMP 加入组

- 3) 配置 IGMP 加入静态组
- (2) 配置 IGMP 查询参数
 - 1) 配置 IGMP 发送查询报文的时间间隔
 - 2) 配置 IGMP 查询的最大反应时间
 - 3) 配置 IGMP 查询的超时时间
- (3) 配置 IGMP 版本
- 3、关闭 IGMP 协议

1. 启动 IGMP 协议

在三层交换机上没有启动 IGMP 协议的专门命令，在相应接口下启动任何一种组播协议，则 IGMP 自动随之启动。

命令	解释
全局配置模式	
ip dvmrp multicast-routing ip pim multicast-routing	启动全局组播协议，是启动 IGMP 协议的必要前提，相应命令的 no 操作关闭组播协议以及 IGMP 协议。（必须）

命令	解释
接口配置模式	
ip dvmrp enable ip pim dense-mode ip pim sparse-mode	启动 IGMP 协议，相应命令的 no 操作关闭 IGMP 协议。（必须）

2. 配置 IGMP 辅助参数

- (1) 配置 IGMP 组 group 参数
 - 1) 配置 IGMP 组过滤条件
 - 2) 配置 IGMP 加入组
 - 3) 配置 IGMP 加入静态组

命令	解释
接口配置模式	
ip igmp access-group {<acl_num acl_name>} no ip igmp access-group	配置接口对 IGMP 组的过滤条件；本命令的 no 操作取消过滤条件。
ip igmp join-group <A.B.C.D > no ip igmp join-group <A.B.C.D >	配置接口加入某个 IGMP 组；本命令的 no 操作取消加入。
ip igmp static-group <A.B.C.D > no ip igmp static -group <A.B.C.D>	配置接口加入某个 IGMP 静态组；本命令的 no 操作取消加入。

(2) 配置 IGMP 查询参数

- 1) 配置 IGMP 发送查询报文的时间间隔

- 2) 配置 IGMP 查询的最大响应时间
- 3) 配置 IGMP 查询的超时时间

命令	解释
接口配置模式	
ip igmp query-interval <time_val> no ip igmp query-interval	配置周期发送 IGMP 查询消息的时间间隔；本命令的 no 操作恢复缺省值。
ip igmp query-max-response-time <time_val> no ip igmp query-max-response-time	配置接口对 IGMP 查询的最大反应时间；本命令的 no 操作恢复缺省值。
ip igmp query-timeout <time_val> no ip igmp query-timeout	配置接口对 IGMP 查询的超时时间；本命令的 no 操作恢复缺省值。

(3) 配置 IGMP 版本

命令	解释
全局配置模式	
ip igmp version <version> no ip igmp version	配置接口上 IGMP 版本；本命令的 no 操作恢复为缺省值。

3. 关闭 IGMP 协议

命令	解释
接口配置模式	
no ip dvmrp enable no ip pim dense-mode no ip pim sparse-mode no ip pim multicast-routing (全局配置模式) no ip pim multicast-routing (全局配置模式)	关闭 IGMP 协议。

1.9.3 IGMP典型案例

如下图，将switchA 和switchB 的以太网端口加入相应的VLAN，并在各VLAN接口上启动PIM-DM。

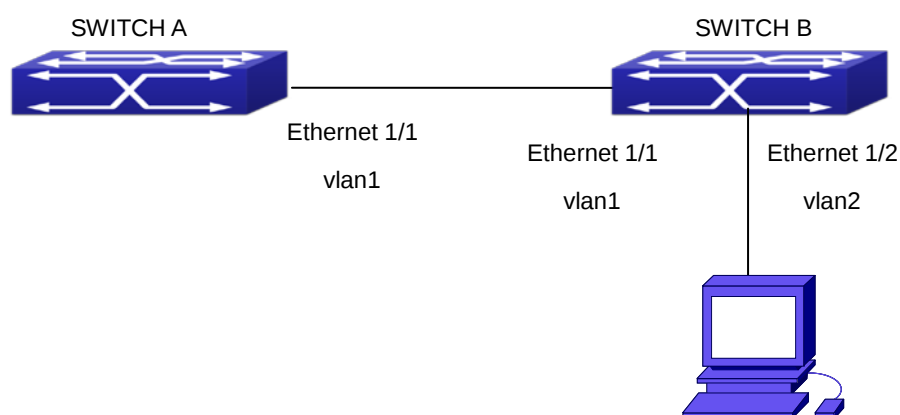


图 1-10 IGMP 网络拓扑示意图

switchA 和 switchB 配置步骤如下：

(1) 配置 SwitchA:

```
Switch(config)#ip pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-If-Vlan1)#ip address 12.1.1.1 255.255.255.0
Switch(Config-If-Vlan1)#ip pim dense-mode
```

(2) 配置 SwitchB:

```
Switch(config)#ip pim multicast-routing
Switch(config)#interface vlan1
Switch(Config-If-Vlan1)#ip address 12.1.1.2 255.255.255.0
Switch(Config-If-Vlan1)#ip pim dense-mode
Switch(Config-If-Vlan1)#exit
Switch(config)#interface vlan2
Switch(Config-If-Vlan1)#ip address 20.1.1.1 255.255.255.0
Switch(Config-If-Vlan2)#ip pim dense-mode
Switch(Config-If-Vlan2)#ip igmp version 3
```

1.9.4 IGMP排错帮助

在配置、使用 IGMP 协议时，可能会由于物理连接、配置错误等原因导致 IGMP 协议未能正常运行。因此，用户应注意以下要点：

- ☞ 首先应该保证物理连接的正确无误；
- ☞ 其次，保证接口和链路协议是 UP（使用 show interface 命令）；
- ☞ 然后，确保在接口上启动一种组播协议；
- ☞ 组播协议需使用单播路由进行 RPF 检查，因此必须首先确保单播路由的正确性。

1.10 IGMP Snooping配置

1.10.1 IGMP Snooping介绍

IGMP (Internet Group Management Protocol) 互联网组管理协议，用于实现IP的组播。IGMP被支持组播的网络设备（如路由器）用来进行主机资格查询，也被想加入某组播组的主机用来通知路由器接收某个组播地址的数据包，而这些都是通过IGMP消息交换来完成的。路由器首先利用一个可寻址到所有主机的组地址（即224.0.0.1）发送一条IGMP主机成员资格查询（IGMP Host Membership Query）消息。若一个主机希望加入某组播组，它就利用该组播组的组地址回应一条IGMP主机成员资格报告（IGMP Host Membership Report）消息。

IGMP Snooping 即 IGMP 侦听。交换机通过 IGMP Snooping 来限制组播流量的泛滥，只把组播流量转发给与组播设备相连的端口。交换机侦听组播路由器和主机之间的 IGMP 消息，根据侦听结果维护组播转发表，而交换机根据组播转发表来决定组播包的转发。

交换机实现了 IGMP Snooping 功能，并且支持 IGMP v3，这样，用户可以用交换机实现 IP 组播。

1.10.2 IGMP Snooping配置任务

1.启动 IGMP Snooping 功能

2.配置 IGMP Snooping

1.启动 IGMP Snooping 功能

命令	解释
全局配置模式	
ip igmp snooping no ip igmp snooping	启动 IGMP Snooping 功能。no 操作关闭全局 IGMP snooping 功能。

2.配置 IGMP Snooping

命令	解释
全局配置模式	
ip igmp snooping vlan <vlan-id> no ip igmp snooping vlan <vlan-id>	启动指定 VLAN 的 IGMP Snooping 功能。 No 操作关闭指定 VLAN 上的 IGMP Snooping。
ip igmp snooping proxy no ip igmp snooping proxy	开启 IGMP Snooping 代理功能，本命令的 no 操作为关闭 IGMP Snooping 代理功能。
ip igmp snooping vlan < vlan-id > limit {group <g_limit> source <s_limit>}	设置 IGMP snooping 可加入组的个数和每个组中源个数的最大值。no 操作恢复默认值。

no ip igmp snooping vlan <vlan-id> limit	
ip igmp snooping vlan <1-4094> interface (ethernet port-channel) IFNAME limit {group <1-65535> source <1-65535>} strategy (replace drop) no ip igmp snooping vlan <1-4094> interface (ethernet port-channel) IFNAME limit group source strategy	设置 IGMP Snooping 端口下可允许加入组的个数和每个组中源个数的最大值，及当达到上限值时的处理策略：包括替换和丢弃。no 操作设置为“无限制”。
ip igmp snooping vlan <vlan-id> l2-general-querier no ip igmp snooping vlan <vlan-id> l2-general-querier	将该 VLAN 设为二层普通查询者，每一个网段推荐配置一个二层普通查询者。no 操作取消二层普通查询者设置。
ip igmp snooping vlan <vlan-id> l2-general-querier-version <version>	该命令配置二层查询者发送普通查询的版本号。
ip igmp snooping vlan <vlan-id> l2-general-querier-source <source>	该命令配置二层查询者发送普通查询的源地址。
ip igmp snooping vlan <vlan-id> mrrouter-port interface <interface -name> no ip igmp snooping vlan <vlan-id> mrrouter-port interface <interface -name>	设置指定 VLAN 内的静态 mrrouter 端口。no 操作取消 mrrouter 端口设置。
ip igmp snooping vlan <vlan-id> mrrouter-port learnpim no ip igmp snooping vlan <vlan-id> mrrouter-port learnpim	打开指定 VLAN 根据 pim 报文学习 mrrouter-port 的功能；本命令的 no 操作为关闭指定 VLAN 根据 pim 报文学习 mrrouter-port 的功能。
ip igmp snooping vlan <vlan-id> mrpt <value> no ip igmp snooping vlan <vlan-id> mrpt	设置 mrrouter 端口存活时间，no 操作恢复默认值。
ip igmp snooping vlan <vlan-id> query-interval <value> no ip igmp snooping vlan <vlan-id> query-interval	设置查询间隔，no 操作恢复默认值。
ip igmp snooping vlan <vlan-id> immediately-leave no ip igmp snooping vlan <vlan-id> immediately-leave	设置指定 VLAN 的 IGMP Snooping 具有快速离开组播组功能，no 操作取消 immediately-leave 设置。

<pre>ip igmp snooping vlan <vlan-id> query-mrsp <value> no ip igmp snooping vlan <vlan-id> query-mrsp</pre>	设置查询的最大响应时间，no 操作恢复默认值。
<pre>ip igmp snooping vlan <vlan-id> query-robustness <value> no ip igmp snooping vlan <vlan-id> query-robustness</pre>	设置查询鲁棒值，no 操作恢复默认值。
<pre>ip igmp snooping vlan <vlan-id> suppression-query-time <value> no ip igmp snooping vlan <vlan-id> suppression-query-time</pre>	设置抑制查询时间值，no 操作恢复默认值。
<pre>ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source< A.B.C.D>] interface [ethernet port-channel] <IFNAME> no ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source< A.B.C.D>] interface [ethernet port-channel] <IFNAME></pre>	设置静态组源，no 操作取消设置的静态组源。
<pre>ip igmp snooping vlan <vlan-id> report source-address <A.B.C.D> no ip igmp snooping vlan <vlan-id> report source-address</pre>	设置转发 IGMP 报文源地址，no 操作取消设置的报文源地址。
<pre>ip igmp snooping vlan <vlan-id> specific-query-mrsp <value> no ip igmp snooping vlan <vlan-id> specific-query-mrspt</pre>	配置特定组/源查询的最大响应时间值，no 操作恢复默认值。

1.10.3 IGMP Snooping 典型案例

案例 1: IGMP Snooping 功能。

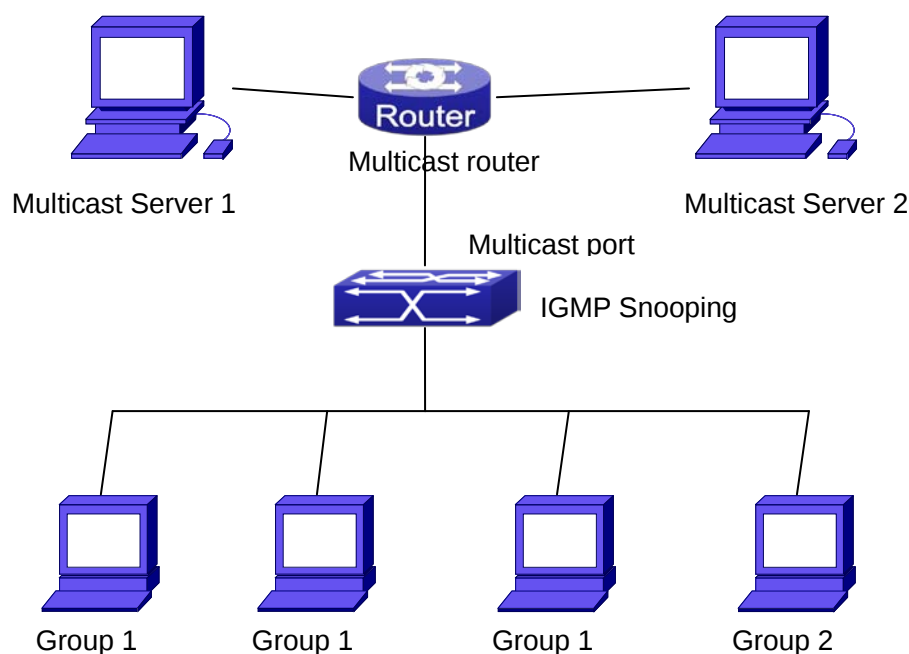


图 1-11 打开交换机 IGMP Snooping 功能图

如图所示，switch 上配置 VLAN 100 包含端口 1、2、6、10、12。四台主机分别连在端口 2、6、10、12 上，组播路由器连在端口 1 上。端口 1 因为与组播路由器相连，会被识别为 MROUTER 端口。假设我们需要在 VLAN 100 上做 IGMP Snooping，缺省情况下，交换机的全局 IGMP Snooping 功能和各 VLAN 上的 IGMP Snooping 功能都不打开。因此，需要打开全局下的 IGMP Snooping 功能，同时在 VLAN 100 上打开 IGMP Snooping，还需要设置 VLAN 100 的端口 1 为 mrouter 端口。如果组播路由器启动了三层组播，则 VLAN 100 的端口 1 被自动识别为 mrouter 端口，不需手动配置。

配置步骤如下：

```
Switch#config
```

```
Switch(config)#ip igmp snooping
```

```
Switch(config)#ip igmp snooping vlan 100
```

```
Switch(config)#ip igmp snooping vlan 100 mrouter-port interface ethernet 1/1
```

组播配置：

假设有两个组播服务器 Multicast Server 1 和 Multicast Server 2，其中组播服务器 1 上提供节目 1，组播服务器 2 上提供节目 2。分别使用组地址 Group1 和 Group 2 四台主机上同时运行组播应用软件，连在端口 2、6、10 上的三台主机播放节目 1，连在端口 12 上的主机播放节目 2。

IGMP Snooping 侦听结果：

VLAN 100 上 IGMP Snooping 建立的组播表显示：其中端口 1、2、6、10 在（Multicasting Server 1， Group1）中，端口 1、12 在（Multicast Server 2， Group 2）中。

四台主机都能正常地收到自己感兴趣的节目，端口 2、6、10 不会收到节目 2 的流量，端口 12 不会收到节目 1 的流量。

“show mac-address-table multicast”命令可以查看 switch B 上的二层组播转发表。注意：224.0.0.1~224.0.0.255 范围内的地址为预留组播地址，所以与这类地址的 MAC 地址（01-00-5e-00-00-xx）相同的组播组地址不应该被使用，因为他们不会下发到二层组播转发表。

案例 2: IGMP L2-general-querier

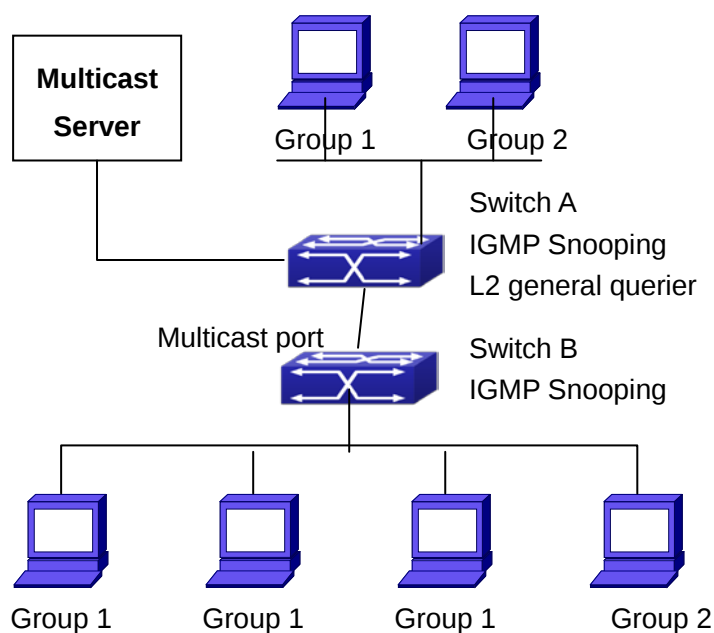


图 1-12 交换机作为 IGMP Querier 功能图

switch B 的配置与案例 1 中交换机相同，交换机 switch A 取代案例 1 中的 Multicast Router。假设其上配置 VLAN 60 包含端口 1、2、10、12。端口 1 连接组播服务器，端口 2 连接 switch B。为了定期发 Query，需要打开全局下的 IGMP Snooping 功能，同时需要执行 IGMP Snooping vlan 60 l2-general-querier，将 VLAN 60 设置成为二层普通查询者。

配置步骤如下：

```
SwitchA#config
```

```
SwitchA(config)#ip igmp snooping
```

```
SwitchA(config)#ip igmp snooping vlan 60
```

```
SwitchA(config)#ip igmp snooping vlan 60 l2-general-querier
```

```
SwitchB#config
```

```
SwitchB(config)#ip igmp snooping
```

```
SwitchB(config)#ip igmp snooping vlan 100
```

```
SwitchB(config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/1
```

组播配置：

同案例 1。

IGMP Snooping 侦听结果：

与案例 1 相似。

案例 3： 与三层组播协议混合运行

我们将案例1中的SWITCH替换为ROUTER，配置与原SWITCH配置相同，组播配置与IGMP snooping侦听结果与案例1相同。在ROUTER上全局启动三层组播(PIM-SM)，同时在VLAN 100上启动PIM SM。(与上层组播路由器使用相同PIM模式)

配置步骤如下：

```
switch#config
```

```
switch(config)#ip pim multicast-routing
```

```
switch(config)#interface vlan 100
```

```
switch(config-if-vlan100)#ip pim sparse-mode
```

此时由于存在三层组播协议，IGMP snooping 不再下发表项，只负责以下几件事情：

- 删除二层组播表项
- 向三层提供端口查询函数，参数为 VLAN，S，G
- 当三层 IGMP 关闭时，重新下发二层组播表项

通过观察三层 IPMC 表项，发现三层组播出入表项仍然可以精确到端口，保证了 IGMP snooping 与三层组播协议的混合运行。

1.10.4 IGMP Snooping排错帮助

在配置、使用 IGMP Snooping 功能时，可能会由于物理连接、配置错误等原因导致 IGMP Snooping 未能正常运行。因此，用户应注意以下要点：

- ☞ 应该保证物理连接的正确无误
- ☞ 保证全局配置模式下 IGMP Snooping 打开（使用 ip igmp snooping）
- ☞ 保证全局配置模式下 VLAN 上配置 IGMP Snooping（使用 ip igmp snooping vlan <vlan-id>）
- ☞ 确保同一网段内存在查询者，并确认是否存在 mrouter
- ☞ 使用 show ip igmp snooping vlan <vid>命令查看 IGMP Snooping 信息是否正确
- ☞ 如果使用检查仍无法解决 IGMP Snooping 的问题，那么请使用 debug igmp snooping 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给本公司技术服务中心

1.11 IGMP Proxy配置

1.11.1 IGMP Proxy介绍

IGMP/MLD proxy是在rfc4605中提出的一种简化的组播末端协议，其核心是在运行环境简单的组播协议末端，不运行复杂的PIM/DVMRP等组播路由协议，通过IGMP/MLD代理的方式与组播协议对话，从而简化在低端设备上的组播实现。

IGMP/MLD协议是用来在组播路由器和客户端间通信的协议，同时也存在组播路由器和客户端两种协议行为，IGMP/MLD代理设备在配置上明确上游接口和下游接口，对于上游接口，协议运行HOST端协议，在下游接口，则运行ROUTER端协议，IGMP/MLD代理交换机把从下游收集的IGMP/MLD加入信息汇聚成HOST端状态，以IGMP/MLD客户端的身份发送加入、离开消息给上层的组播路由器，从而实现不需组播路由协议的简单组播成员关系。

IGMP proxy 功能与 PIM 及 DVMRP的功能是互斥的。

1.11.2 IGMP Proxy配置任务

1. 启动 IGMP Proxy 功能
2. 在不同接口上打开 IGMP Proxy 的上游接口和下游接口开关
3. 配置 IGMP Proxy

1. 启动 IGMP Proxy 功能

命令	解释
全局配置模式	
ip igmp proxy	启动 IGMP Proxy 功能。本命令的 no 操作关闭全局 IGMP Proxy 功能。
no ip igmp proxy	

2. 在不同接口上打开 IGMP Proxy 的上游接口和下游接口开关

命令	解释
接口配置模式	
ip igmp proxy upstream	启动 IGMP Proxy 上游接口功能。本命令的 no 操作关闭 IGMP Proxy 上游接口功能。
no ip igmp proxy upstream	
ip igmp proxy downstream	启动 IGMP Proxy 下游接口功能。本命令的 no 操作关闭 IGMP Proxy 下游接口功能。
no ip igmp proxy downstream	

3. 配置 IGMP Proxy 辅助参数

命令	解释
全局配置模式	
ip igmp proxy limit {group <1-500>}	设置 IGMP Proxy 上游接口可加入组的个数

source <1-500>} no ip igmp proxy limit	和每个组中源个数的最大值。本命令的 no 操作恢复默认值。
ip igmp proxy unsolicited-report interval <1-5> no ip igmp proxy unsolicited-report interval	设置 IGMP Proxy 上游接口状态改变报告重传时间间隔。本命令的 no 操作恢复默认值。
ip igmp proxy unsolicited-report robustness <2-10> no ip igmp proxy unsolicited-report robustness	设置 IGMP Proxy 上游接口状态改变报告重传个数。本命令的 no 操作恢复默认值。
ip igmp proxy aggregate no ip igmp proxy aggregate	设置 IGMP Proxy 非查询者下游接口也可以作为下发表项的出接口。本命令的 no 操作恢复默认设置。
ip multicast ssm range <1-99> ip multicast ssm default no ip mulitcast ssm	设置 IGMP Proxy SSM 组播组地址范围；本命令的 no 操作删除配置的 igmp proxy ssm 组播组。
ip igmp proxy multicast-source no ip igmp proxy multicast-source	设置指定下游接口作为组播数据源接口；本命令的 no 操作取消该下游接口作为组播数据源接口。

1.11.3 IGMP Proxy 举例

案例 1：IGMP Proxy 功能。

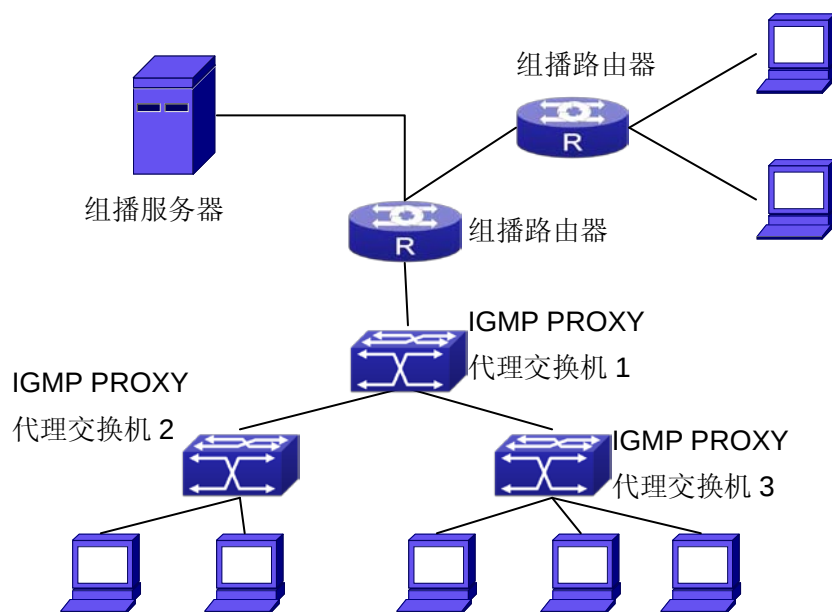


图 1-13 打开交换机 IGMP Proxy 功能图

如图所示，IGMP PROXY 代理交换机以树型拓扑存在于简单的网络环境中，组播流量沿着树枝从上游接口向下游扩散，而 igmp 组播成员报告沿着树枝从下游向上游汇聚，通知上游接口。三台 IGMP PROXY 代理交换机以树型拓扑组织，分别有一个接口与上层路由器相连，一个或多个下游接口或者直接跟主机相连，或者跟 IGMP PROXY 代理交换机的上游接口相连。

配置步骤如下：

```
Switch#config
Switch(config)#ip igmp proxy
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp proxy upstream
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ip igmp proxy downstream
```

组播配置：

假设有组播服务器上提供组播地址 224.1.1.1 的节目，网络末端有主机点播该节目，igmp 组播成员报告通知 IGMP PROXY 代理交换机 2 和 3 的下游接口，IGMP PROXY 代理交换机 2 和 3 的上游接口汇聚该组播成员关系，再向 IGMP PROXY 代理交换机 1 点播，通知上层组播路由器。当有组播流量到达时，IGMP PROXY 代理交换机的上游接口将组播成员关系下发，组播流量按照 IGMP PROXY 下发的出接口转发。

案例 2：IGMP Proxy 下游接口组播数据源功能。

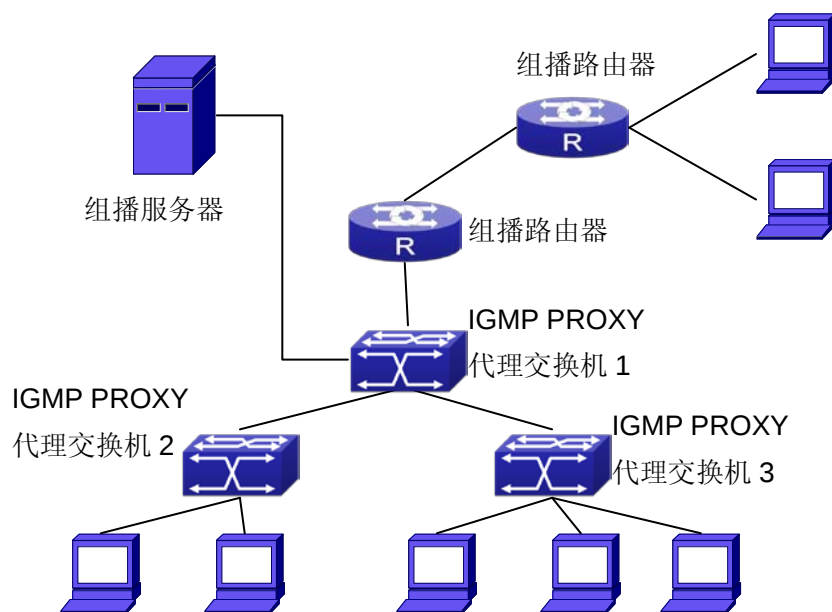


图 1-14 打开交换机 IGMP Prox 下游接口组播源功能图

如图所示，IGMP PROXY 代理交换机以树型拓扑存在于简单的网络环境中，组播源位于代理交换机 1 的下游，组播流量到达时，默认上游接口作为出接口，沿着树枝从下游接口向上游和其他下游接口扩散。三台 IGMP PROXY 代理交换机以树型拓扑组织，分别有一个接口与上层路由器相连，一个或多个下游接口或者直接跟主机相连，或者跟 IGMP PROXY 代理交换机的上游接口相连。

配置步骤如下：

IGMP PROXY 代理交换机 1 配置：

```
Switch#config
Switch(config)#ip igmp proxy
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp proxy upstream
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ip igmp proxy downstream
Switch(Config-if-Vlan2)#ip igmp proxy multicast-source
```

组播路由器 1 配置：

```
Switch#config
Switch(config)#ip pim multicast
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip pim sparse-mode
Switch(Config-if-Vlan1)#ip pim bsr-border
```

组播配置：

假设有组播服务器上提供组播地址 224.1.1.1 的节目，网络末端有主机点播该节目，igmp 组播成员报告通知 IGMP PROXY 代理交换机 2 和 3 的下游接口，IGMP PROXY 代理交换机 2 和 3 的上游接口汇聚该组播成员关系，再向 IGMP PROXY 代理交换机 1 点播，通知上层组播路由器。当有组播流量到达时，IGMP PROXY 代理交换机的上游接口将组播成员关系下发，下发接口中默认加入上游接口，组播流量按照 IGMP PROXY 下发的出接口转发。组播路由器收到代理服务器发出的组播流量，认为所有该接口接收的组播数据源均为直连，而确定 DR 和 ORIGINATOR 的身份，组播数据按照 PIM 协议继续转发。

1.11.4 IGMP Proxy排错帮助

在配置、使用 IGMP Proxy 功能时，可能会由于物理连接、配置错误等原因导致 IGMP Proxy 未能正常运行。因此，用户应注意以下要点：

- ☞ 应该保证物理连接的正确无误；
- ☞ 保证全局配置模式下 IGMP Proxy 打开（使用 `ip igmp proxy`）；
- ☞ 保证接口配置模式下一个上游接口和至少一个下游接口（使用 `ip igmp proxy upstream`, `ip igmp proxy downstream`）；
- ☞ 使用 `show ip igmp proxy` 命令查看 IGMP Proxy 配置信息是否正确。

如果使用检查仍无法解决 IGMP Proxy 的问题，那么请使用 `debug igmp proxy` 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给本公司技术服务中心。

第2章 IPv6 组播协议

2.1 PIM-DM6

2.1.1 PIM-DM6 介绍

PIM-DM6 (Protocol Independent Multicast, Dense Mode, 协议独立组播—密集模式) 即与协议无关组播-密模式的IPv6版本, 属于密集模式的组播路由协议, 适用于小型网络, 在这种网络环境下, 组播组的成员相对比较密集。与用于IPv4版本的PIM-DM版本相比较, 除了所使用的地址为IPv6地址以外, 没有其它的区别。因此, 在本章中对于PIM-DM和PIM-DM6不加区别, 凡是使用PIM-DM而不加说明的都是指PIM-DM的IPv6版本。

由于IPv6网络还在发展中, 有时网络中存在不支持IPv6组播的网络环境, 这就需要通过隧道进行IPv6组播的操作, 所以我们的PIM-DM6支持在配置隧道上的配置, 以IPv4单播的方式穿过不支持IPv6组播的网络。

PIM-DM 的工作过程可以概括为: 邻居发现、扩散—剪枝过程、嫁接阶段。

1. 邻居发现

PIM-DM 路由器刚开始启动时, 需要使用Hello报文来发现邻居。运行PIM-DM的各网络节点之间使用Hello报文保持联系。PIM-DM Hello报文是周期性发送的。

2. 扩散—剪枝过程 (Flooding&Prune)

PIM-DM 假设网络上的所有主机都准备接收组播数据。当某组播源S开始向组播组G发送数据时, 在路由器接收到组播报文后, 首先根据单播路由表进行RPF检查, 如果检查通过, 路由器创建一个 (S, G) 表项, 然后将组播报文向网络上所有下游PIM-DM节点转发 (Flooding)。如果没有通过RPF检查, 即组播报文是从错误的接口输入, 则将该报文丢弃。经过这个过程, 在PIM-DM组播域内, 每个节点都会创建一个 (S, G) 表项。如果下游节点没有组播组成员, 则向上游节点发剪枝 (Prune) 消息, 通知上游节点不用再转发该组播组数据。上游节点收到剪枝消息后, 就将相应的接口从其组播转发表项 (S, G) 对应的输出接口列表中删除, 这就建立了一个以源S为根的SPT (Shortest Path Tree, SPT) 树。剪枝过程最先由叶子路由器发起。

3. RPF检查

PIM-DM采用RPF检查, 利用现存的单播路由表构建一棵从数据源始发的组播转发树。当一个组播包到达时, 路由器首先判断到达路径的正确性。如果到达接口是单播路由指示的通往组播源的接口, 就认为这个组播包是从正确路径而来; 否则, 将组播包作为冗余报文丢弃。作为路径判断依据的单播路由信息可以来源于任何一种单播路由协议, 如RIP、OSPF 等发现的路由信息, 而不依赖于特定的单播路由协议。

4. Assert机制

如果处于一个LAN网段上的两台组播路由器A和B，各自有到组播源S的接收途径，它们在接收到组播源S发出的组播数据报文以后，都会向LAN上转发该组播报文，这时，下游节点组播路由器C就会收到两份相同的组播报文。路由器检测到这种情况后，需要通过Assert机制来选定一个唯一的转发者。通过发送Assert报文，选出一条最优的转发路径，如果两条或两条以上路径的优先级和开销相同，则选择IP地址大的节点作为该（S，G）项的上游邻居，由它负责该（S，G）组播报文的转发。

5. 嫁接（Graft）

当被剪枝的下游节点需要恢复到转发状态时，该节点使用嫁接报文通知上游节点恢复组播数据转发。

6. PIM-DM6的状态刷新

为了减少PIM-DM6周期性的扩散-剪枝，PIM-DM6协议最新版本提供了一个选项（option），它将从组播源的第一跳路由器开始，周期性的向下面广播（S，G）状态刷新消息以完成状态刷新。当下游PIM路由器收到（S，G）状态刷新消息，它就将剪枝计时器复位，终止剪枝计时器超时，从而即保证了网络的时效性，避免了周期性的扩散-剪枝过程。

2.1.2 PIM-DM6 配置任务序列

- 1、启动 PIM-DM（必须）
- 2、配置静态组播表项（可选）
- 3、配置 PIM-DM 辅助参数（可选）
 - (1) 配置 PIM-DM 接口参数
 - 1) 配置 PIM-DM hello 报文间隔时间
 - 2) 配置 PIM-DM state-refresh 报文间隔时间
 - 3) 配置边缘接口
 - 4) 配置管理边界
- 4、关闭 PIM-DM 协议

1. 启动 PIM-DM 协议

在三层交换机上运行 PIM-DM 路由协议的基本配置很简单，需全局配置模式下打开 PIM 组播开关，然后在相应接口下打开 PIM-DM 开关即可。

命令	解释
全局配置模式	
ipv6 pim multicast-routing	使各个接口上的 PIM-DM 协议进入使能状态（但真正在接口上开始 PIM-DM 协议，还需下面的命令）。

然后在接口上打开 PIM-SM 开关

命令	解释
接口配置模式	

ipv6 pim dense-mode	启动本接口 PIM-DM 协议。（必须）
----------------------------	----------------------

2. 配置静态组播表项

命令	解释
全局配置模式	
ipv6 mroute <X:X::X:X> <X:X::X:X> <ifname> <.ifname> no ipv6 mroute <X:X::X:X> <X:X::X:X> [<ifname> <.ifname>]	配置静态组播表项 其 no 命令删除静态组播表项或其出接口。

3. 配置 PIM-DM 辅助参数

（1）配置 PIM-DM 接口参数

1）配置 PIM-DM hello 报文间隔时间

命令	解释
接口配置模式	
ipv6 pim hello-interval <interval> no ipv6 pim hello-interval	配置接口 PIM-DM hello 报文间隔时间；本命令的 no 操作恢复为缺省值。

2）配置 PIM-DM state-refresh 报文间隔时间

命令	解释
接口配置模式	
ipv6 pim state-refresh origination-interval no ipv6 pim state-refresh origination-interval	配置接口 PIM-DM state-refresh 报文间隔时间；本命令的 no 操作恢复为缺省值。

3）配置边缘接口

命令	解释
接口配置模式	
ipv6 pim bsr-border no ipv6 pim bsr-border	配置接口为 PIM-DM6 边缘接口，边缘接口上，STATE REFRESH 相关消息不向该接口发送也不从该接口接收，连接的网络被认为都是该接口的直连网络。本命令的 no 操作取消该配置。

4）配置管理边界

命令	解释
接口配置模式	

<code>ipv6 pim scope-border <500-599> <acl_name> no ipv6 pim scope-border</code>	配置 PIM-DM6 管理边界和使用的 ACL。组播数据不向 SCOPE-BORDER 扩散，默认的情形下，认为 ffx0::/13 的范围为管理组范围，若配置了 ACL，则 ACL permit 的范围为管理组范围。acl_name 应当是 IPV6 标准 ACL 名。本命令的 no 操作取消该配置。
--	--

4. 关闭 PIM-DM 协议

命令	解释
接口配置模式	
<code>no ipv6 pim dense-mode</code>	在接口上关闭 PIM-DM 协议。
全局配置模式	
<code>no ipv6 pim multicast-routing</code>	全局关闭 PIM-DM 协议。

2.1.3 PIM-DM6 典型案例

如下图，将SwitchA，switchB的以太网接口加入到相应的VLAN中，并在各VLAN接口上启动PIM-DM协议。如果VLAN内同时配置了IGMP SNOOPING，则组播流量能精确到端口，而不在整个VLAN内泛洪。

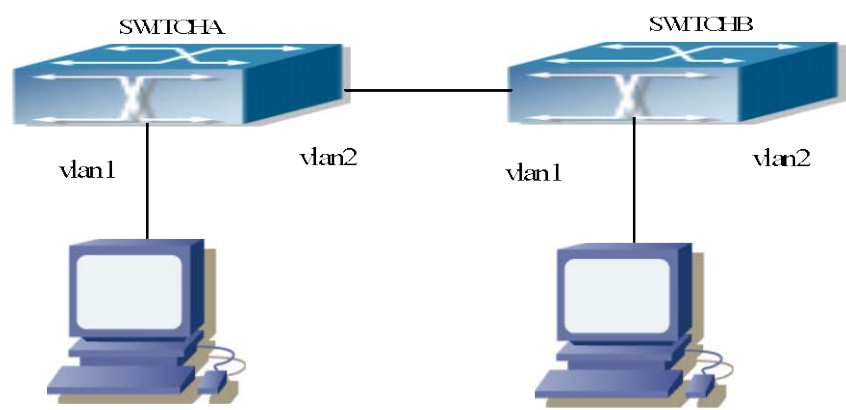


图 2-1 PIM-DM 典型环境

SwitchA 和SwitchB配置步骤如下：

(1) 配置SwitchA:

```
Switch (config)#ipv6 pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)# ipv6 address 2000:10:1:1::1/64
Switch(Config-if-Vlan1)# ipv6 pim dense-mode
Switch(Config-if-Vlan1)#exit
```

```
Switch (config)#interface vlan2
Switch(Config-if-Vlan2)# ipv6 address 2000:12:1:1::1/64
Switch(Config-if-Vlan2)# ipv6 pim dense-mode
(2) 配置SwitchB:
Switch (config)#ip pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)# ipv6 address 2000:12:1:1::2/64
Switch(Config-if-Vlan1)# ipv6 pim dense-mode
Switch(Config-if-Vlan1)#exit
Switch (config)#interface vlan 2
Switch(Config-if-Vlan2)# ipv6 address 2000:20:1:1::1/64
Switch(Config-if-Vlan2)# ipv6 pim dense-mode
```

2.1.4 PIM-DM6 排错帮助

在配置、使用 PIM-DM 协议时，可能会由于物理连接、配置错误等原因导致 PIM-DM 协议未能正常运行。因此，用户应注意以下要点：

- ☞ 应该保证物理连接的正确无误；
- ☞ 保证接口和链路协议是 UP（使用 show interface 命令）；
- ☞ 保证全局配置模式下打开 PIM 协议(使用 ipv6 pim multicast-routing)
- ☞ 在接口上启动 PIM-DM 协议（使用 ipv6 pim dense-mode 命令）。

组播协议需使用单播路由进行 RPF 检查，因此必须首先确保单播路由的正确性；如果使用检查仍无法解决 PIM-DM 的问题，那么请使用 debug ipv6 pim 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给本公司技术服务中心。

2.2 PIM-SM6

2.2.1 PIM-SM6 介绍

PIM-SM6（Protocol Independent Multicast, Sparse Mode）即与协议无关组播-稀疏模式的IPv6版本，属于稀疏模式的组播路由协议，主要用于组成员分布相对分散、范围较广、大规模的网络。与用于IPv4版本的PIM-SM版本相比较，除了所使用的地址为IPv6地址以外，没有其它的区别。因此，在本章中对于PIM-SM和PIM-SM6不加区别，凡是使用PIM-SM而不加说明的都是指PIM-SM的IPv6版本。与密集模式的扩散—剪枝不同，PIM-SM协议假定所有的主机都不需要接收组播数据包，只有主机明确指定需要时，PIM-SM路由器才向它转发组播数据包。

PIM-SM通过设置汇聚点RP（Rendezvous Point）和自举路由器BSR（Bootstrap Router），向所有PIM-SM路由器通告组播信息，并利用路由器的加入/剪枝信息，建立起基

于RP的共享树RPT（RP-rooted shared tree）。从而减少数据报文和控制报文占用的网络带宽，降低路由器的处理开销。组播数据沿着共享树流到该组播组成员所在的网段，当数据流量达到一定程度，组播数据流可以切换到基于源的最短路径树SPT，以减少网络延迟。

PIM-SM不依赖于特定的单播路由协议，而是使用现存的单播路由表进行RPF检查。

由于IPv6网络还在发展中，有时网络中存在不支持IPv6组播的网络环境，这就需要通过隧道进行IPv6组播的操作，所以我们的PIM-SM6支持在配置隧道上的配置，以IPv4单播的方式穿过不支持IPv6组播的网络。

1. PIM-SM 工作原理

PIM-SM的工作过程主要有：邻居发现、RP共享树（RPT）的生成、组播源注册、SPT切换等。其中，邻居发现机制与PIM-DM相同，这里不再介绍。

(1) RP 共享树（RPT）的生成

当主机加入一个组播组G时，与该主机直接相连的叶子路由器通过IGMP报文了解到有组播组G的接收者，就为组播组G计算出对应的汇聚点RP，然后向朝着RP方向的上一级节点发送加入组播组的消息（join 消息）。从叶子路由器到RP之间途经的每个路由器都会在转发表中生成（*, G）表项，表示由任意源发出的，发送至组播组G的，都适用于该表项。当RP收到发往组播组G的报文后，报文就会沿着已经建立好的路径到达叶子路由器，进而到达主机。这样就生成了以RP为根的RPT。

(2) 组播源注册

当组播源S向组播组G发送了一个组播报文时，与其直接相连的PIM-SM组播路由器接收到该报文以后，就负责将该组播报文封装成注册报文，单播给对应的RP。如果一个网段上有多个PIM-SM组播路由器，这时候将由指定路由器DR（Designated Router）负责发送该组播报文。

(3) SPT 切换

当组播路由器发现从RP发来的目的地址为G的组播报文的速率超过了阈值时，组播路由器就向朝着源S的上一级节点发送加入消息，导致RPT向SPT的切换。

2. PIM-SM 配置前准备工作

(1) 配置候选 RP

在PIM-SM网络中，可以存在多个RP（候选RP），每个候选RP（Candidate-RP, C-RP）负责转发目的地址在一定范围内的组播报文。配置多个候选RP可以实现RP负载分担。候选RP之间没有主次之分，所有的组播路由器收到BSR通告的候选RP消息后，根据相同的算法计算出与某一组播组对应的RP。

注意，一个RP可以为多个组播组服务，也可以为所有组播组服务。每个组播组在任意时刻，只能唯一地对应一个RP，不能同时对应多个RP。

(2) 配置 BSR

BSR 是PIM-SM 网络里的管理核心，它负责收集候选RP发来的信息，并把它们广播出去。

一个网络内部只能有一个BSR，但可以配置多个候选BSR（Candidate-BSR, C-BSR）。这样，一旦某个BSR发生故障后，能够切换到另外一个。C-BSR通过自动选举产生BSR。

2.2.2 PIM-SM6 配置任务序列

- 1、启动 PIM-SM（必须）
- 2、配置静态组播表项（可选）
- 3、配置 PIM-SM 辅助参数（可选）
 - (1) 配置 PIM-SM 接口参数
 - 1) 配置 PIM-SM hello 报文间隔时间
 - 2) 配置 PIM-SM hello 报文 holdtime 时间
 - 3) 配置 PIM-SM 邻居访问列表
 - 4) 配置接口为 PIM-SM6 边缘接口
 - 5) 配置接口为 PIM-SM6 管理边界
 - (2) 配置 PIM-SM 全局参数
 - 1) 配置交换机作为候选 BSR
 - 2) 配置交换机作为候选 RP
 - 3) 配置静态 RP
 - 4) 配置内核组播路由缓存时间
- 4、关闭 PIM-SM 协议

1. 启动 PIM-SM 协议

在三层交换机上运行 PIM-SM 路由协议的基本配置很简单，需全局配置模式下打开 PIM 组播开关，然后在相应接口下打开 PIM-SM 开关即可。

命令	解释
全局配置模式	
[no] ipv6 pim multicast-routing	使各个接口上的 PIM-SM 协议进入使能状态(但真正在接口上开始 PIM-SM 协议，还需下面的命令)，本命令的 no 操作关闭所有接口上的 PIM-SM 协议。（必须）

然后在接口上打开 PIM-SM 开关

命令	解释
接口配置模式	
[no] ipv6 pim sparse-mode [passive]	启动本接口 PIM-SM 协议，本命令的 no 操作关闭本接口 PIM-SM 协议。（必须）

2. 配置静态组播表项

命令	解释
全局配置模式	

ipv6 mroute <X:X::X:X> <X:X::X:X> <ifname> <.ifname> no ipv6 mroute <X:X::X:X> <X:X::X:X> [<ifname> <.ifname>]	配置静态组播表项，其 no 命令删除静态组播表项或其出接口。
---	--------------------------------

3. 配置 PIM-SM 辅助参数

(1) 配置 PIM-SM 接口参数

1) 配置 PIM-SM hello 报文间隔时间

命令	解释
接口配置模式	
ipv6 pim hello-interval < interval> no ipv6 pim hello-interval	配置接口 PIM-SM hello 报文间隔时间；本命令的 no 操作恢复为缺省值。

2) 配置 PIM-SM hello 报文 holdtime 时间

命令	解释
接口配置模式	
ipv6 pim hello-holdtime <value> no ipv6 pim hello-holdtime	配置接口 PIM-SM hello 报文中的 holdtime 域的值；本命令的 no 操作恢复为缺省值。

3) 配置 PIM-SM 邻居访问列表

命令	解释
接口配置模式	
ipv6 pim neighbor-filter <access-list-name> no ipv6 pim neighbor-filter <access-list-name>	配置邻居访问列表。如果被列表过滤，如果已经同此邻居建立连接，则此连接马上被切断，如果没有建立连接，则这个连接不能建立。

4) 配置边缘接口

命令	解释
接口配置模式	
ipv6 pim bsr-border no ipv6 pim bsr-border	配置接口为 PIM-SM6 边缘接口，边缘接口上，BSR 相关消息不向该接口发送也不从该接口接收，连接的网络被认为都是该接口的直连网络。本命令的 no 操作取消该配置。

5) 配置管理边界

命令	解释
接口配置模式	

<pre> ipv6 pim scope-border <500-599> <acl_name> no ipv6 pim scope-border </pre>	配置 PIM-DM6 管理边界和使用的 ACL。组播数据不向 SCOPE-BORDER 扩散，默认的情形下，认为 ff00::/13 的范围为管理组范围，若配置了 ACL，则 ACL permit 的范围为管理组范围。acl_name 应当是 IPV6 标准 ACL 名。本命令的 no 操作取消该配置。
---	---

(2) 配置 PIM-SM 全局参数

1) 配置交换机作为候选 BSR

命令	解释
全局配置模式	
<pre> ipv6 pim bsr-candidate {vlan <vlan_id> <ifname> tunnel <1-50> [hash-mask-length] [priority] no ipv6 pim bsr-candidate{vlan <vlan_id> <ifname> tunnel <1-50> [<hash-mask-length>] [<priority>] </pre>	该命令为全局候选 BSR 配置命令，用于配置 PIM-SM 候选 BSR 的信息，以用于同其它候选 BSR 竞争 BSR 路由器；本命令的 no 操作为取消候选 BSR 的配置。

2) 配置交换机作为候选 RP

命令	解释
全局配置模式	
<pre> ipv6 pim rp-candidate {vlan<vlan-id> loopback<index> <ifname>} [<group range>] [<priority>] no ipv6 pim rp-candidate </pre>	该命令为全局候选 RP 配置命令，用于配置 PIM-SM 候选 RP 的信息，以用于同其它候选 RP 竞争 RP 路由器；本命令的 no 操作为取消候选 RP 的配置。

3) 配置静态 RP

命令	解释
全局配置模式	
<pre> ipv6 pim rp-address <rp-address> [<group-range>] no ipv6 pim rp-address <rp-address> {all <group-range>} </pre>	该命令为全局或某个组播地址范围的组播组配置静态 RP，本命令的 no 操作为取消静态 RP 的配置。

4) 配置内核组播路由缓存时间

命令	解释
全局配置模式	

ipv6 multicast unresolved-cache aging-time <value> no ipv6 multicast unresolved-cache aging-time	配置内核组播路由缓存时间；本命令的 no 操作恢复为缺省值。
---	--------------------------------

4.关闭 PIM-SM 协议

命令	解释
接口配置模式	
no ipv6 pim sparse-mode	关闭 PIM-SM 协议。
全局配置模式	
no ipv6 pim multicast-routing	全局关闭 PIM-SM 协议。

2.2.3 PIM-SM6 典型案例

如下图所示，将switchA，switchB，switchC，switchD的以太网接口加入到相应VLAN中，并在各VLAN接口上启动PIM-SM协议。如果VLAN内同时配置了IGMP SNOOPING，则组播流量能精确到端口，而不在整个VLAN内泛洪。

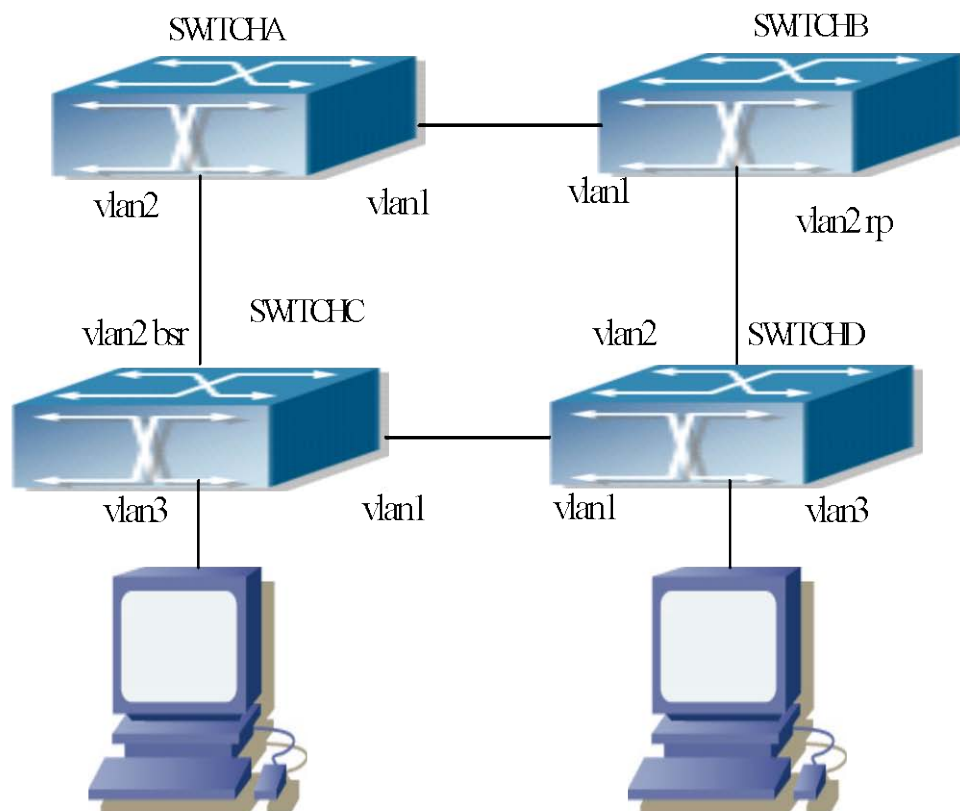


图 2-2 PIM-SM 典型环境

SwitchA 和 SwitchB, switchC, switchD 配置步骤如下:

(1) 配置 SwitchA:

```
Switch(config)#ipv6 pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-If-Vlan1)# ipv6 address 2000:12:1:1::1/64
Switch(Config-If-Vlan1)# ipv6 pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (config)#interface vlan 2
Switch(Config-If-Vlan2)# ipv6 address 2000:13:1:1::1/64
Switch(Config-If-Vlan2)# ipv6 pim sparse-mode
```

(2) 配置 SwitchB:

```
Switch(config)#ipv6 pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-If-Vlan1)# ipv6 address 2000:12:1:1::2/64
Switch(Config-If-Vlan1)# ipv6 pim sparse-mode
```

```
Switch(Config-If-Vlan1)#exit
Switch (config)#interface vlan 2
Switch(Config-If-Vlan2)# ipv6 address 2000:24:1:1::2/64
Switch(Config-If-Vlan2)# ipv6 pim sparse-mode
Switch(Config-If-Vlan2)# exit
Switch (config)# ipv6 pim rp-candidate vlan2
```

(3) 配置 SwitchC:

```
Switch(config)#ipv6 pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-If-Vlan1)# ipv6 address 2000:34:1:1::3/64
Switch(Config-If-Vlan1)# ipv6 pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (config)#interface vlan 2
Switch(Config-If-Vlan2)# ipv6 address 2000:13:1:1::3/64
Switch(Config-If-Vlan2)# ipv6 pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch (config)#interface vlan 3
Switch(Config-If-Vlan3)# ipv6 address 2000:30:1:1::1/64
Switch(Config-If-Vlan3)# ipv6 pim sparse-mode
Switch(Config-If-Vlan3)# exit
Switch (config)# ipv6 pim bsr-candidate vlan2 30 10
```

(4) 配置 SwitchD:

```
Switch(config)#ipv6 pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-If-Vlan1)# ipv6 address 2000:34:1:1::4/64
Switch(Config-If-Vlan1)# ipv6 pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (config)#interface vlan 2
Switch(Config-If-Vlan2)# ipv6 address 2000:24:1:1::4/64
Switch(Config-If-Vlan2)# ipv6 pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch (config)#interface vlan 3
Switch(Config-If-Vlan3)# ipv6 address 2000:40:1:1::1/64
Switch(Config-If-Vlan3)# ipv6 pim sparse-mode
```

2.2.4 PIM-SM6 排错帮助

在配置、使用 PIM-SM 协议时，可能会由于物理连接、配置错误等原因导致 PIM-SM 协议未能正常运行。因此，用户应注意以下要点：

- ☞ 首先应该保证物理连接的正确无误；
- ☞ 其次，保证接口和链路协议是 UP（使用 `show interface` 命令）；
- ☞ 组播协议需使用单播路由进行 RPF 检查，因此必须首先确保单播路由的正确性；
- ☞ PIM-SM 协议需要有 rp 和 bsr 的支持，所以首先使用 `show ipv6 pim bsr-router`，看是否有 bsr 信息，如果不存在，则需要查看是否有通向 bsr 的单播路由；
- ☞ 使用 `show ipv6 pim rp-hash` 命令查看 rp 信息是否正确，如果没有 rp 信息，也要检查单播路由。

如果使用检查仍无法解决 PIM-SM 的问题，那么请使用 `debug ipv6 pim/ debug ipv6 pim bsr` 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给本公司技术服务中心。

2.3 ANYCAST RP v6 配置

2.3.1 ANYCAST RP v6 介绍

基于 PIM 协议的 Anycast RP v6 是一种为了让 RP 失效能够尽快恢复而提供冗余的技术，Anycast-RP 地址通常是配置在 loopback 接口上的地址。

Anycast RP v6 的核心思想是在整个网络上配置的 RP 地址，存在于多台组播路由器上（通常的情况是在各个提供 ANYCAST RP 的设备上都使用 LOOPBACK 接口，并配置 RP 地址在这个接口上，使用最长的掩码），而单播路由算法将决定了 PIM 路由器总是能找到离自己最近的 RP，因此对于比较大的网络提供了更短更快的找到 RP 的路径。而一旦正在使用的某一个 RP 失效，单播路由算法将保证 PIM 路由器很快找到新的 RP 路径，从而使组播服务迅速恢复。多个 RP 会出现新的问题，即如果组播源和接收者注册到不同的 RP，会导致有的接收者不能接收到组播源数据（注册报文显然只会青睐离自己的最近的 RP）。因此，为了在各 RP 间保持联络，Anycast RP 规定离组播源最近的 RP 在收到注册报文时应将源注册信息转发通知给其他 RP，保证所有 RP 上的加入者都可以找到该组播源。

基于 PIM 协议的 Anycast RP 具体实现方法是：在每个配置了 Anycast RP 的交换机上维护一份 ANYCAST RP 的列表，并使用另一个地址作为他们之间互相识别的标志，在一台 Anycast RP 设备收到注册消息后，以标志自己的地址作为源地址向其它 Anycast RP 设备发送注册消息，以达到让其它设备也知道本源的目的。

2.3.2 ANYCAST RP v6 配置任务

- 1.启动 ANYCAST RP v6 功能
- 2.配置 ANYCAST RP v6

1.启动 ANYCAST RP v6 功能

命令	解释
全局配置模式	
<code>ipv6 pim anycast-rp</code>	启动 ANYCAST RP 功能。（必须）

no ipv6 pim anycast-rp	no 操作关闭全局 ANYCAST RP 功能。
-------------------------------	--------------------------

2.配置 ANYCAST RP v6

(1) 配置候选 RP

命令	解释
全局配置模式	
<pre> ipv6 pim rp-candidate {vlan<vlan-id> loopback<index> <ifname>} [<A:B::C:D>] [<priority>] no ipv6 pim rp-candidate </pre>	目前 PIM6-SM 已允许配置 Loopback 接口作为候选 RP。(必须) 需要注意的是, ANYCAST RP 协议可以配置 Loopback 接口或普通三层 VLAN 接口作为候选 RP。为使网络中 PIM 路由器找到 RP 位置, 应将候选 RP 接口加入到路由中。 no 操作取消本路由器候选 RP 配置。

(2) 配置 self-rp-address (本 RP 通信地址)

命令	解释
全局配置模式	
<pre> ipv6 pim anycast-rp self-rp-address A:B::C:D no ipv6 pim anycast-rp self-rp-address </pre>	在本路由器（作为 RP）上配置本路由器的 self-rp-address。该地址唯一标志本路由器, 用于与其他 RPs 之间的通讯。(必须) self-rp-address 具体作用有两个方面: 1 当本路由器（作为 RP）收到从 DR 单播过来的注册报文, 需要将该注册报文向网络中其他 RP 转发, 使得网络中所有 RP 获得源 (S,G) 状态。转发时, 本路由器修改注册报文源地址为 self-rp-address。 2 当本路由器（作为 RP）收到从其他 RP 单播转发过来的注册报文, 如注册报文目的地址为本路由器 self-rp-address, 则建立 (S,G) 状态并反方向发送注册中止报文, 注册中止报文目的地址即注册报文的源地址。 注意: self-rp-address 应为本路由器上某个三层接口地址, 但在配置时我们允许此接口当前不存在。self-rp-address 是唯一的。 no 操作取消本路由器用于与其他 RP 通信的 self-rp-address。

(3) 配置 other-rp-address (其他 RP 通信地址)

命令	解释
全局配置模式	
ipv6 pim anycast-rp <anycast-rp-addr> <other-rp-addr> no ipv6 pim anycast-rp <anycast-rp-addr> <other-rp-addr>	在本路由器（作为 RP）上配置 anycast-rp-addr 地址。该单播地址实际上就是在网络中多个 RP 上配置的 RP 地址，对应候选 RP 接口(或者 Loopback 接口)的地址。 anycast-rp-addr 具体作用有： 1 允许配置多个 anycast-rp-addr 地址，只有与当前配置的候选 RP 接口地址相同的 anycast-rp-addr 地址生效。此时对应该 anycast-rp-addr 地址的 other-rp-address 也才会生效。 2 配置时我们允许 anycast-rp-addr 对应的接口当前不存在。 在本路由器（作为 RP）上配置与本路由器通讯的其他 RP 的 other-rp-address。该单播地址标志其他 RP，用于与本地路由器之间的通讯。 other-rp-address 具体作用有两个方面： 1 当本路由器（作为 RP）收到从 DR 单播过来的注册报文，需要将该注册报文向网络中其他 RP 转发，使得网络中所有 RP 获得源（S，G）状态。转发时，本路由器修改注册报文目的地址为 other-rp-address。 2 对应一个 anycast-rp-addr 可以配置多个 other-rp-address，当收到 DR 单播过来的注册报文，依次向这些其他 RP 转发。 no 操作取消与本路由器通信的某个 other-rp-address。

2.3.3 ANYCAST RP v6 典型案例

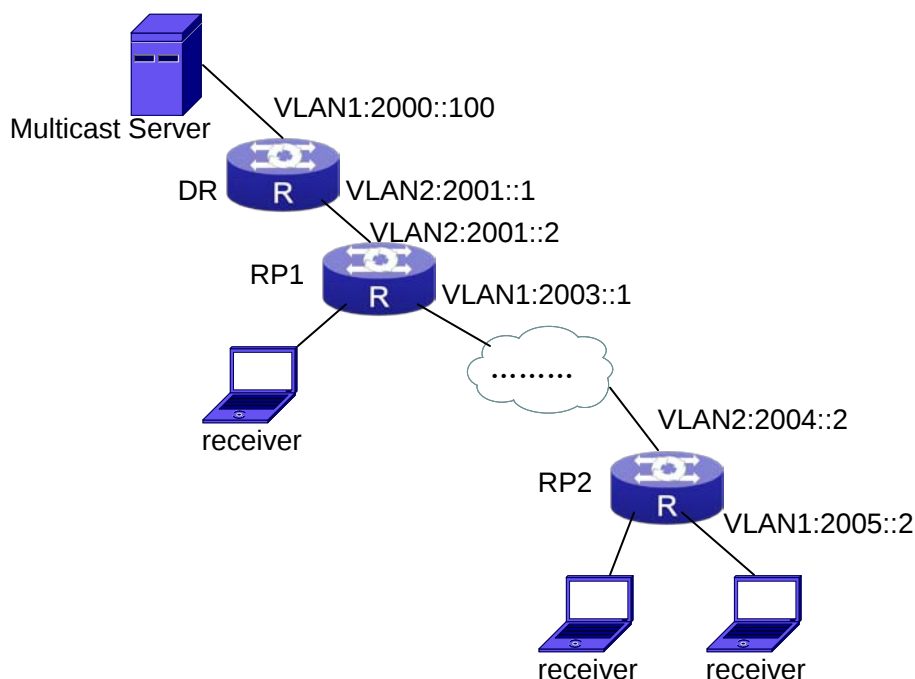


图 2-3 路由器 ANYCAST RP v6 功能

配置步骤如下：

RP1 配置：

```
Switch#config
Switch(config)#interface loopback 1
Switch(Config-if-Loopback1)#ipv6 address 2006::1/128
Switch(Config-if-Loopback1)#exit
Switch(config)#ipv6 pim rp-candidate loopback1
Switch(config)#ipv6 pim bsr-candidate vlan 1
Switch(config)#ipv6 pim multicast-routing
Switch(config)#ipv6 pim anycast-rp
Switch(config)#ipv6 pim anycast-rp self-rp-address 2003::1
Switch(config)#ipv6 pim anycast-rp 2006::1 2004::2
```

RP2 配置：

```
Switch#config
Switch(config)#interface loopback 1
Switch(Config-if-Loopback1)#ipv6 address 2006::1/128
Switch(Config-if-Loopback1)#exit
Switch(config)#ipv6 pim rp-candidate loopback1
Switch(config)#ipv6 pim multicast-routing
Switch(config)#ipv6 pim anycast-rp
Switch(config)#ipv6 pim anycast-rp self-rp-address 2004::2
```

```
Switch(config)#ipv6 pim anycast-rp 2006::1 2003::1
```

需要注意，为发布 loopback 接口路由，如使用 MBGP4+协议，可使用 network 命令；如使用 RIPvng 协议，可使用 route 命令。

2.3.4 ANYCAST RP v6 排错帮助

在配置、使用 ANYCAST RP v6 功能时，可能会由于物理连接、配置错误等原因导致 ANYCAST RP 未能正常运行。因此，用户应注意以下要点：

- ☞ 应该保证物理连接的正确无误
- ☞ 保证 PIM-SM6 协议正确运行
- ☞ 保证全局配置模式下 ANYCAST RP 打开。
- ☞ 保证全局配置模式下 self-rp-address 配置正确
- ☞ 保证全局配置模式下 other-rp-address 配置正确
- ☞ 保证各接口路由正确添加，包括作为 RP 的 loopback 接口也要正确加入路由
- ☞ 使用 show ipv6 pim anycast rp status 命令查看 ANYCAST RP 配置信息是否正确

如果使用检查仍无法解决 ANYCAST RP 的问题，那么请使用 debug ipv6 pim anycast-rp 调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给本公司技术服务中心。

2.4 PIM-SSM6

2.4.1 PIM-SSM6 介绍

源指定组播(PIM-SSM6)是一种区别于传统组播的新的业务模式，它使用组播组地址和组播源地址来同时标志一个组播会话。SSM保留了传统PIM-SM6模式中的主机显示加入组播组的高效性，但是跳过了PIM-SM6模式中的共享树和RP规程。SSM6直接建立由(S,G)标志的spt树，其中G表示组播组的地址，S表示发向组播组G的特定组播源的地址。SSM6的一个(S，G)对也被称为一个频道。SSM特别适用于点到多点的组播服务，如网络体育频道，网络新闻频道等业务。在缺省情况下，SSM6组播组地址范围限制在IPV6地址范围：ff3x::/32内，但是可以根据需要对地址进行扩展。

PIM-DM6的环境中也支持PIM-SSM6。

2.4.2 PIM-SSM6 配置任务序列

命令	解释
全局配置模式	
ipv6 pim ssm {default range <access-list-number >}	该命令配置pim ssm 组播组地址范围；本命令的no 操作删除配置的pim ssm 组播组
no ipv6 pim ssm	

2.4.3 PIM-SSM6 典型案例

如下图所示，将switchA，switchB，switchC，switchD的以太网接口加入到相应VLAN中，并在各VLAN接口上启动PIM-SM6协议，或者PIM-DM6协议，全局启动PIM-SSM6。本例以PIM-SM6协议为例。

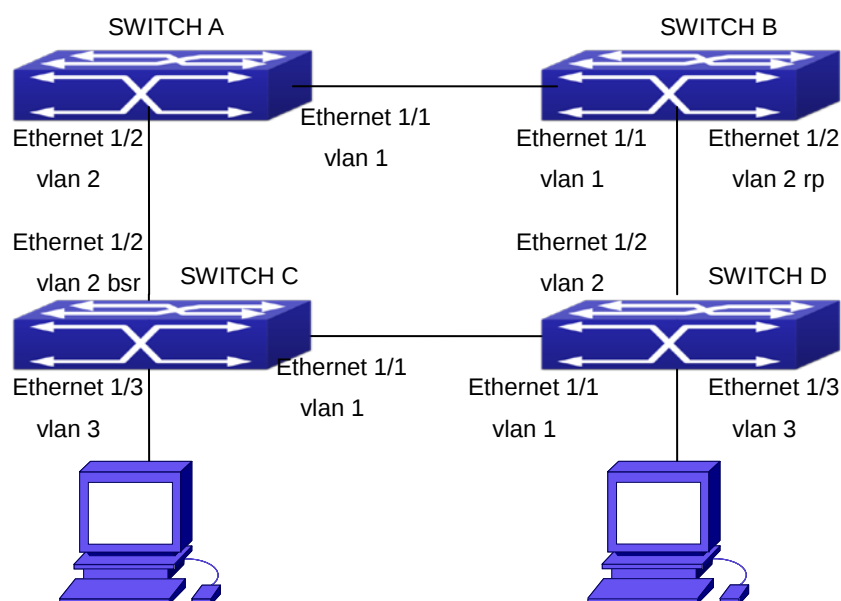


图 2-4 PIM-SSM 典型环境

switchA 和 switchB，switchC，switchD 配置步骤如下：

(1) 配置 switchA:

```
Switch(config)#ipv6 pim multicast-routing
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)# ipv6 address 2000:12:1:1::1/64
Switch(Config-If-Vlan1)# ipv6 pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-If-Vlan2)# ipv6 address 2000:13:1:1::1/64
Switch(Config-If-Vlan2)# ipv6 pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch(config)#ipv6 access-list 500 permit ff1e::1/64
Switch(config)#ip multicast ssm range 500
```

(2) 配置 switchB:

```
Switch(config)#ipv6 pim multicast-routing
```

```
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)# ipv6 address 2000:12:1:1::2/64
Switch(Config-If-Vlan1)# ipv6 pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-If-Vlan2)# ipv6 address 2000:24:1:1::2/64
Switch(Config-If-Vlan2)# ipv6 pim sparse-mode
Switch(Config-If-Vlan2)# exit
Switch(config)# ipv6 pim rp-candidate vlan2
Switch(config)#ipv6 access-list 500 permit ff1e::1/64
Switch(config)#ip multicast ssm range 500
```

(3) 配置 SwitchC:

```
Switch(config)#ipv6 pim multicast-routing
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)# ipv6 address 2000:34:1:1::3/64
Switch(Config-If-Vlan1)# ipv6 pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-If-Vlan2)# ipv6 address 2000:13:1:1::3/64
Switch(Config-If-Vlan2)# ipv6 pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch(config)#interface vlan 3
Switch(Config-If-Vlan3)# ipv6 address 2000:30:1:1::1/64
Switch(Config-If-Vlan3)# ipv6 pim sparse-mode
Switch(Config-If-Vlan3)# exit
Switch(config)# ipv6 pim bsr-candidate vlan2 30 10
Switch(config)#ipv6 access-list 500 permit ff1e::1/64
Switch(config)#ip multicast ssm range 500
```

(4) 配置 SwitchD:

```
Switch(config)#ipv6 pim multicast-routing
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)# ipv6 address 2000:34:1:1::4/64
Switch(Config-If-Vlan1)# ipv6 pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-If-Vlan2)# ipv6 address 2000:24:1:1::4/64
Switch(Config-If-Vlan2)# ipv6 pim sparse-mode
Switch(Config-If-Vlan2)#exit
```

```
Switch(config)#interface vlan 3
Switch(Config-If-Vlan3)# ipv6 address 2000:40:1:1::1/64
Switch(Config-If-Vlan3)# ipv6 pim sparse-mode
Switch(Config-If-Vlan3)#exit
Switch(config)#ipv6 access-list 500 permit ff1e::1/64
Switch(config)#ip multicast ssm range 500
```

2.4.4 PIM-SSM6 排错帮助

在配置、使用 PIM-SSM6 协议时，可能会由于物理连接、配置错误等原因导致 PIM-SSM6 协议未能正常运行。因此，用户应注意以下要点：

- ☞ 应该保证物理连接的正确无误；
- ☞ 保证接口和链路协议是 UP（使用 show interface 命令）；
- ☞ 保证全局配置模式下 PIM6 协议打开（使用 ipv6 pim multicast-routing）；
- ☞ 保证接口上配置 PIM-SSM6（使用 ipv6 pim sparse-mode）；
- ☞ 保证全局模式下配置 SSM6；
- ☞ 组播协议需使用单播路由进行 RPF 检查，因此必须首先确保单播路由的正确性。

如果使用检查仍无法解决问题，那么请使用 debug ipv6 pim event/debug ipv6 pim packet 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给本公司技术服务中心。

2.5 IPv6 DCSCM

2.5.1 IPv6 DCSCM介绍

IPv6 DCSCM（Destination Control and Source Control Multicast）技术主要包含三个方面，即组播信源可控、组播用户可控及面向服务优先级的策略组播。

IPv6 DCSCM 的组播信源可控技术主要采取以下的方式进行：

1. 在边缘交换机上，如果配置的源受控组播，只有指定源发出的指定组的组播数据才能通过。
2. 对于处于 PIM-SM 核心地位的 RP 交换机，对于指定源及指定组以外的 REGISTER 信息，直接发送 REGISTER_STOP，而不允许建立表项。（该任务在 PIM-SM 模块中实现）。

IPv6 DCSCM 技术的组播用户可控技术的实现基于对用户发出的 MLD report 报文的控制，因此进行控制的模块是 MLD snooping 和 MLD 模块，其控制逻辑包括以下三种，即根据发送报文的 VLAN+MAC 地址进行控制，根据发送报文的 IP 地址进行控制和根据报文进入的端口进行控制。其中 MLD snooping 可以同时使用上述三种方式进行控制，而 MLD 模块由于处于三层，仅针对发送报文的 IP 地址进行控制。

IPV6 DCSCM 技术的面向服务优先级的策略组播采用下述的方式：对于限定范围的组播数据，在接入端就设置用户指定的优先级，使得数据在干道端口（TRUNK）上以更高的优先级发送，从而在整个网络上保证其以用户指定的优先级传送。

2.5.2 IPv6 DCSCM配置任务序列

- 1. 源受控的配置
- 2. 目的受控的配置
- 3. 组播策略的配置

1. 源受控的配置

源受控的配置分三个部分，首先是全局启动源受控，全局启动源受控的命令如下：

命令	解释
全局配置模式	
ipv6 multicast source-control(必须) no ipv6 multicast source-control	全局启动源控制，本命令的 no 操作全局关闭源控制。值得注意的是，全局启动源控制后，所有组播报文都默认丢弃。所有源控制配置都要在全局启动后才可以进行，而只有关闭所有已经配置的规则后，才可以全局关闭源控制。

其次是配置源控制的规则，它使用与 ACL 相同的方式配置，使用 8000—8099 的 ACL 号，每个规则号最多可配置 10 个规则，值得注意的是，这些规则是有顺序的，先配置的在最前面，一旦所配置的规则得到匹配，其后面的规则将不会起作用，所以全局允许的规则一定要配置在最后。其命令如下

命令	解释
全局配置模式	
[no] ipv6 access-list <8000-8099> {deny permit} {{<source/M>} {host-source <source-host-ip>} any-source} {{<destination/M> } {host-destination <destination-host-ip>} any-destination}	用于配置源受控使用的规则，该规则只有应用到指定的端口上时才可以生效。使用其 NO 形式可以删除指定的规则。

最后是把配置的规则配置到指定的端口上。

注意：由于配置的规则要占据硬件的表项，配置过多的规则可能导致由于底层表项满而配置失败，因此建议用户尽可能使用简单的规则。配置命令如下：

命令	解释
端口配置模式	

[no] ipv6 multicast source-control access-group <8000-8099>	用于把源受控使用的规则配置到端口上，其 NO 形式取消该配置。
--	---------------------------------

2. 目的受控的配置

目的受控的配置与源受控配置相似，也是分三个步骤。

首先要全局打开目的受控，由于目的受控要防止未获授权的用户接收到组播数据，因此配置全局目的受控后，交换机对收到的组播数据不再广播，因此，应当避免在启动了目的受控的交换机上同一 VLAN 内连接两台或以上的其它三层交换机。其配置命令如下：

命令	解释
全局配置模式	
multicast destination-control(必须)	全局启动 IPV4 和 IPV6 目的控制，本命令的 no 操作全局关闭目的控制。所有其它的配置都只有在全局启动后才能生效。

其次是配置目的控制规则，它与源控制相似，只是使用 9000—10099 的 ACL 号。

命令	解释
全局配置模式	
[no] ipv6 access-list <9000-10099> {deny permit} {{<source/M>}}{host-source <source-host-ip>}}any-source} {{<destination/M>}}{host-destination <destination-host-ip>}}any-destination}	用于配置源受控使用的规则，该规则只有应用到指定的源 IP 或 VLAN-MAC、端口上时才可以生效。使用其 NO 形式可以删除指定的规则

最后要把该规则配置到指定的源 IP、源 VLAN MAC 或指定端口上。这里需要注意的是，由于上面所说的情况，只有在启动 MLD-SNOOPING 的情况下才可以全面使用这些规则，而如果没有启动 MLD-SNOOPING，则只有源 IP 的规则才能在 MLD 协议使用。其配置命令如下：

命令	解释
端口配置模式	
[no] ipv6 multicast destination-control access-group <9000-10099>	用于把目的受控使用的规则配置到端口上，其 NO 形式取消该配置。
全局配置模式	
[no] ipv6 multicast destination-control <1-4094> <macaddr> access-group <9000-10099>	用于把目的受控使用的规则配置到指定的 VLAN-MAC 上，其 NO 形式取消该配置。
[no] ipv6 multicast destination-control <IPADDRESS/M> access-group <9000-10099>	用于把目的受控使用的规则配置到指定的源 IPv6 地址/掩码上，其 NO 形式取消该配置。

3. 组播策略的配置

组播策略使用为指定的组播数据指定优先级的方式达到保证特定用户需求的效果，值得

注意的是组播数据只有在干道端口上传输才能保证数据一直得到重点照顾。其配置很简单，只有一个命令，即为指定的组播设定优先级，命令如下：

命令	解释
全局配置模式	
[no] ipv6 multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority>	配置组播策略，为特定范围的源、组指定优先级，范围为<0-7>。

2.5.3 IPv6 DCSCM典型案例

1. 源受控

为了防止一台边缘交换机随意发布组播数据，我们在边缘交换机上配置，只有在端口 Ethernet1/4 的交换机才允许发送组播数据，且数据的组必须是 ff1e::1。而上连端口 Ethernet1/25 可以不受限制的转发组播数据，则我们可以进行如下配置。

```
Switch(config)#ipv6 access-list 8000 permit any-source ff1e::1
Switch(config)#ipv6 access-list 8001 permit any any
Switch(config)#ipv6 multicast source-control
Switch(config)#interface Ethernet1/4
Switch(Config-If-Ethernet1/4)#ipv6 multicast source-control access-group 8000
Switch(config)#interface Ethernet1/25
Switch(Config-If-Ethernet1/25)#ipv6 multicast source-control access-group 8001
```

2. 目的受控

我们要限制地址在 fe80::203:fff:fe01:228a/64 网段的用户不能加入 ff1e::1/64 的组，我们可以做如下配置：

首先在其所在的 VLAN(这里认为是 VLAN2)内要启动 MLD snooping。

```
Switch(config)#ipv6 mld snooping
Switch(config)#ipv6 mld snooping vlan 2
```

然后配置相关的目的控制访问列表，并配置指定的 IPv6 地址使用该访问列表。

```
Switch(config)#ipv6 access-list 9000 deny any ff1e::1/64
Switch(config)#ipv6 access-list 9000 permit any any
Switch(config)#ipv6 multicast destination-control
Switch(config)#ipv6 multicast destination-control fe80::203:fff:fe01:228a/64 access-group 9000
```

这样，该网段的用户就只能加入 2ff1e::1/64 以外的组了。

3. 组播策略

服务器 2008::1 正在组 ff1e::1 上发布重要的组播数据，我们可在其接入交换机上配置如下：

```
Switch(config)#ipv6 multicast policy 2008::1/128 ff1e::1/128 cos 4
```

这样该组播流在通过本交换机的 TRUNK 端口通向其它交换机时，将拥有值为 4 的优先

级（通常这已经比较高了，更高的可能是协议数据了，若设置更高的优先级，在该组播数据太多时，有可能造成交换机协议行为的不正常）。

2.5.4 IPv6 DCSCM排错帮助

IPv6 DCSCM 模块本身作用与 ACL 相似，发生问题通常与不当的配置有关，请您详细阅读上面的说明。

注：12GT、12GB、4GX24TX 板卡不支持组播源受控。

2.6 MLD

2.6.1 MLD介绍

MLD(Multicast Listener Discovery)是服务于IPv6组播的组播组成员（接受者）发现协议，类似于IPv4组播应用中的IGMP协议，其中MLD协议版本1类似于IGMP协议的版本2，MLD协议版本2类似于IGMP协议的版本3，我们目前实现了MLDv2。

参与IPv6 组播的主机可以在任意位置、任意时间、成员总数不受限制地加入或退出组播组。组播交换机不需要也不可能保存所有主机的成员关系，它只是通过MLD 协议了解每个接口连接的网段上是否存在某个组播组的接收者，即组成员。而主机方只需要保存自己加入了哪些组播组。

MLD 在主机与路由器之间是不对称的：主机需要响应组播交换机的MLD查询报文，即以成员资格报告报文响应；交换机周期性发送成员资格查询报文，然后根据收到的响应报文确定某个特定组在自己所在子网上是否有主机加入，并且当收到主机的退出组的报告时，发出特定组的查询，以确定某个特定组是否已无成员存在。

MLD协议的协议报文可以分为三种类型，即Query，Report和Done（对应于IGMPv2的Leave）。与IGMPV2一样，其Query报文包括了普通查询和特定组查询两种。其普通查询使用所有主机的组播地址FF02::1作为目的地址，而组地址填充为0，其特定查询使用其组地址作为目的地址。MLD的组播地址使用130、131、132作为数据类型，分别表示上述的三种报文。其它的逻辑与IGMPv2也基本相同。

MLDv2增加了V2的report类型，其组播地址使用FF02::16,并使用143作为数据类型，其它逻辑与IGMPV3相同。

2.6.2 MLD配置任务序列

- 1、启动 MLD（必须）
- 2、配置 MLD 辅助参数（可选）
 - （1）配置 MLD 组 group 参数
 - 1) 配置 MLD 组过滤条件

- 2) 配置 MLD 加入组
- 3) 配置 MLD 加入静态组
- (2) 配置 MLD 查询参数
 - 1) 配置 MLD 发送查询报文的时间间隔
 - 2) 配置 MLD 查询的最大反应时间
 - 3) 配置 MLD 查询的超时时间
- (3) 配置 MLD 版本
- 3、关闭 MLD 协议

1. 启动 MLD 协议

在三层交换机上没有启动 MLD 协议的专门命令，在相应接口下启动任何一种 IPv6 组播协议，则 MLD 自动随之启动。

命令	解释
全局配置模式	
ipv6 pim multicast-routing	启动全局 IPv6 组播协议，是启动 MLD 协议的必要前提，相应命令的 no 操作关闭 ipv6 组播协议以及 MLD 协议。（必须）

命令	解释
接口配置模式	
ipv6 pim dense-mode ipv6 pim sparse-mode	启动 MLD 协议，相应命令的 no 操作关闭 MLD 协议。（必须）

2. 配置 MLD 辅助参数

(1) 配置 MLD 组 group 参数

- 1) 配置 MLD 组过滤条件
- 2) 配置 MLD 加入组
- 3) 配置 MLD 加入静态组

命令	解释
接口配置模式	
ipv6 mld access-group <acl_name> no ipv6 mld access-group	配置接口对 MLD 组的过滤条件；本命令的 no 操作取消过滤条件。

ipv6 mld join-group <address> no ipv6 mld join-group <address> ipv6 mld join-group <address> mode <include exclude> source <.X:X::X:X> no ipv6 mld join-group <X:X::X:X> source <.X:X::X:X>	配置接口加入某个 MLD 组或组源；本命令的 no 操作取消加入。
ipv6 mld static-group <group_address> [source <source_address>] no ipv6 mld static-group <group_address> [source <source_address>]	配置接口加入某个 IGMP 静态组或组源；本命令的 no 操作取消加入。

(2) 配置 MLD 查询参数

- 1) 配置 MLD 发送查询报文的时间间隔
- 2) 配置 MLD 查询的最大响应时间
- 3) 配置 MLD 查询的超时时间

命令	解释
接口配置模式	
ipv6 mld query-interval <time_val> no ipv6 mld query-interval	配置周期发送 MLD 查询消息的时间间隔；本命令的 no 操作恢复缺省值。
ipv6 mld query-max-response-time <time_val> no ipv6 mld query-max-response-time	配置接口对 MLD 查询的最大反应时间；本命令的 no 操作恢复缺省值。
ipv6 mld query-timeout <time_val> no ipv6 mld query-timeout	配置接口对 MLD 查询的超时时间；本命令的 no 操作恢复缺省值。

(3) 配置 MLD 版本

命令	解释
全局配置模式	
ipv6 mld version <version> no ipv6 mld version	配置接口上 MLD 版本；本命令的 no 操作恢复为缺省值。

3. 关闭 MLD 协议

命令	解释
接口配置模式	
no ipv6 pim dense-mode no ipv6 pim sparse-mode no ipv6 pim multicast-routing (全局配置模式)	关闭 MLD 协议。

2.6.3 MLD典型案例

如下图，将SwitchA 和SwitchB 的以太网端口加入相应的VLAN，并在各VLAN接口上启动PIM6。

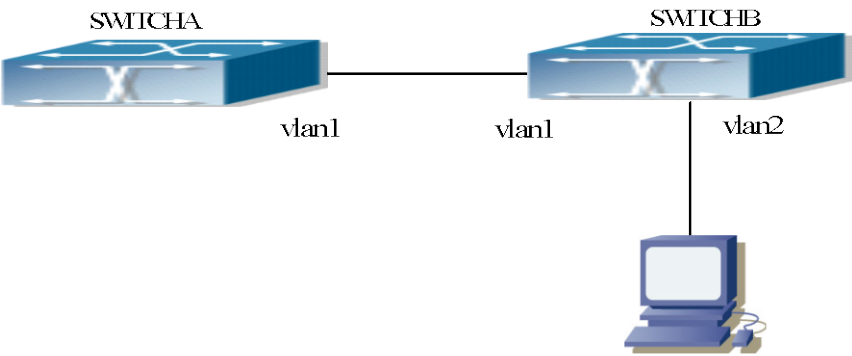


图 2-5 MLD 网络拓扑示意图

SwitchA 和 SwitchB 配置步骤如下：

(1) 配置 SwitchA:

```
Switch(config)#ipv6 pim multicast-routing
Switch(config)#ipv6 pim rp-address 3FFE::1
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)#ipv6 address 3FFE::1/64
Switch(Config-If-Vlan1)#ipv6 pim sparse-mode
```

(2) 配置 SwitchB:

```
Switch(config)#ipv6 pim multicast-routing
Switch(config)#ipv6 pim rp-address 3FFE::1
Switch(config)#interface vlan1
Switch(Config-If-Vlan1)#ipv6 address 3FFE::2/64
Switch(Config-If-Vlan1)#ipv6 pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch(config)#interface vlan2
```

```
Switch(Config-If-Vlan2)#ipv6 address 3FFA::1/64
Switch(Config-If-Vlan2)#ipv6 pim sparse-mode
Switch(Config-If-Vlan2)#ipv6 mld query-timeout 150
```

2.6.4 MLD排错帮助

在配置、使用 MLD 协议时，可能会由于物理连接、配置错误等原因导致 MLD 协议未能正常运行。因此，用户应注意以下要点：

- ☞ 首先应该保证物理连接的正确无误；
- ☞ 其次，保证接口和链路协议是 UP（使用 show interface 命令）；
- ☞ 然后，确保在接口上启动一种组播协议；
- ☞ 注意保证同网段上各路由器定时器时间是一致的，通常我们建议您使用默认的设置；
- ☞ 组播协议需使用单播路由进行 RPF 检查，因此必须首先确保单播路由的正确性。

如果使用检查仍无法解决 MLD 的问题，那么请使用 debug ipv6 mld event/packet 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给本公司技术服务中心。

2.7 MLD Snooping

2.7.1 MLD Snooping介绍

MLD（Multicast Listener Discovery）组播接听者发现协议，用于实现IPv6的组播。MLD被支持组播的网络设备（如路由器）用来进行组播接听者发现，也被想加入某组播组的接听者用来通知路由器接收某个组播地址的数据包，而这些都是通过MLD消息交换来完成的。路由器首先利用一个可寻址到所有接听者的组播地址（即ff02::1）发送一条MLD组播接听者查询（Multicast listener Query）消息。若一个接听者希望加入某组播地址，它就利用该组播地址的地址回应一条MLD接听者报告（Multicast listener Report）消息。

MLD Snooping即MLD侦听。交换机通过MLD Snooping来限制组播流量的泛滥，只把组播流量转发给与组播设备相连的端口。交换机侦听组播路由器和接听者之间的MLD消息，根据侦听结果维护组播转发表，而交换机根据组播转发表来决定组播包的转发。

交换机实现了MLD Snooping功能，并且支持MLD v2，这样，用户可以用交换机实现IPv6组播。

2.7.2 MLD Snooping配置任务

- 1.启动MLD Snooping功能
- 2.配置MLD Snooping

1.启动MLD Snooping功能

命令	解释
----	----

全局配置模式	
ipv6 mld snooping no ipv6 mld snooping	启动全局MLD Snooping功能。no操作关闭全局MLD Snooping功能。

2.配置MLD Snooping

命令	解释
全局配置模式	
ipv6 mld snooping vlan <vlan-id> no ipv6 mld snooping vlan <vlan-id>	启动指定VLAN的MLD Snooping功能。 no 操作 关 闭 指 定 VLAN 上 的 MLD Snooping。
ipv6 mld snooping vlan <vlan-id> limit {group <g_limit> source <s_limit>} no ipv6 mld snooping vlan <vlan-id> limit	设置MLD Snooping可加入组的个数和每个组中源个数的最大值。no操作恢复默认值。
ipv6 mld snooping vlan <vlan-id> l2-general-querier no ipv6 mld snooping vlan <vlan-id> l2-general-querier	将该VLAN设为二层普通查询者，每一个网段推荐配置一个二层普通查询者。no操作取消二层普通查询者设置。
ipv6 mld snooping vlan <vlan-id> mrouter-port interface <interface -name> no ipv6 mld snooping vlan <vlan-id> mrouter-port interface <interface -name>	设置指定VLAN内的静态mrouter端口。 no操作取消mrouter端口设置。
ipv6 mld snooping vlan <vlan-id> mrouter-port learnpim6 no ipv6 mld snooping vlan <vlan-id> mrouter-port learnpim6	打开指定VLAN根据pimv6报文学习mrouter-port的功能；本命令的no操作作为关闭指定VLAN根据pimv6报文学习mrouter-port的功能。
ipv6 mld snooping vlan <vlan-id> mrpt <value> no ipv6 mld snooping vlan <vlan-id> mrpt	设置mrouter端口存活时间，no操作恢复默认值。
ipv6 mld snooping vlan <vlan-id> query-interval <value> no ipv6 mld snooping vlan <vlan-id> query-interval	设置查询间隔，no操作恢复默认值。
ipv6 mld snooping vlan <vlan-id> immediate-leave no ipv6 mld snooping vlan <vlan-id> immediate-leave	设置指定VLAN的MLD Snooping具有快速离开组播组功能，no操作取消immediate-leave设置。
ipv6 mld snooping vlan <vlan-id> query-mrsp <value> no ipv6 mld snooping vlan <vlan-id> query-mrsp	设置查询的最大响应时间，no操作恢复默认值。

<code>ipv6 mld snooping vlan <vlan-id> query-robustness <value> no ipv6 mld snooping vlan <vlan-id> query-robustness</code>	设置查询鲁棒值，no操作恢复默认值。
<code>ipv6 mld snooping vlan <vlan-id> suppression-query-time <value> no ipv6 mld snooping vlan <vlan-id> suppression-query-time</code>	设置抑制查询时间值，no操作恢复默认值。
<code>ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source <X:X::X:X>] interface [ethernet port-channel] <IFNAME> no ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source <X:X::X:X>] interface [ethernet port-channel] <IFNAME></code>	设置静态组源，no 操作取消设置的静态组源

2.7.3 MLD Snooping典型案例

案例1：MLD Snooping功能。

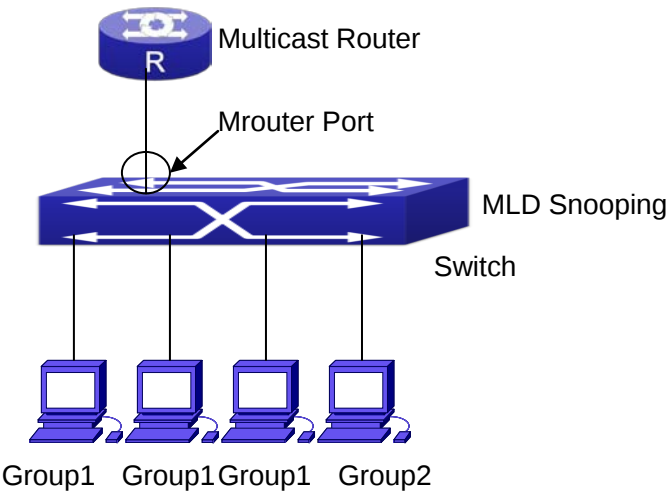


图 2-6 打开交换机 MLD Snooping 功能图

如图所示，switch上配置VLAN 100包含端口1、2、6、10、12。四台主机分别连在端口2、6、10、12上，组播路由器连在端口1上。假设我们需要在VLAN 100上配置MLD Snooping，缺省情况下，交换机的全局MLD Snooping功能和各VLAN上的MLD Snooping功能都不打开。因此，需要打开全局下的MLD Snooping功能，同时在VLAN 100上打开MLD Snooping，还需要设置VLAN 100的端口1为mrouter端口。

配置步骤如下：

```
switch#config
```

```
switch (config)#ipv6 mld snooping
```

```
switch (config)#ipv6 mld snooping vlan 100
```

```
switch (config)#ipv6 mld snooping vlan 100 mrouter-port interface ethernet 1/1
```

组播配置：

假设有两个组播服务器Multicast Server 1和Multicast Server 2，其中组播服务器1上提供节目1、节目2，组播服务器2上提供节目3，分别使用组地址Group1，Group2和Group 3。四台主机上同时运行组播应用软件，连在端口2、6上的两台主机播放节目1，连在端口10上的主机播放节目2，连在端口12上的主机播放节目3。

MLD Snooping侦听结果：

VLAN 100上MLD Snooping建立的组播表显示：其中端口1、2、6在（Multicasting Server 1， Group1）中，端口 1、10在（Multicast Server 1, Group 2）中，端口1、12在（Multicast Server2, Group 3）中。

四台主机都能正常地收到自己感兴趣的节目，端口2、6不会收到节目2和节目3的流量，端口10不会收到节目1和节目3的流量，端口12不会收到节目1和节目2的流量。

案例2：MLD L2-general-querier

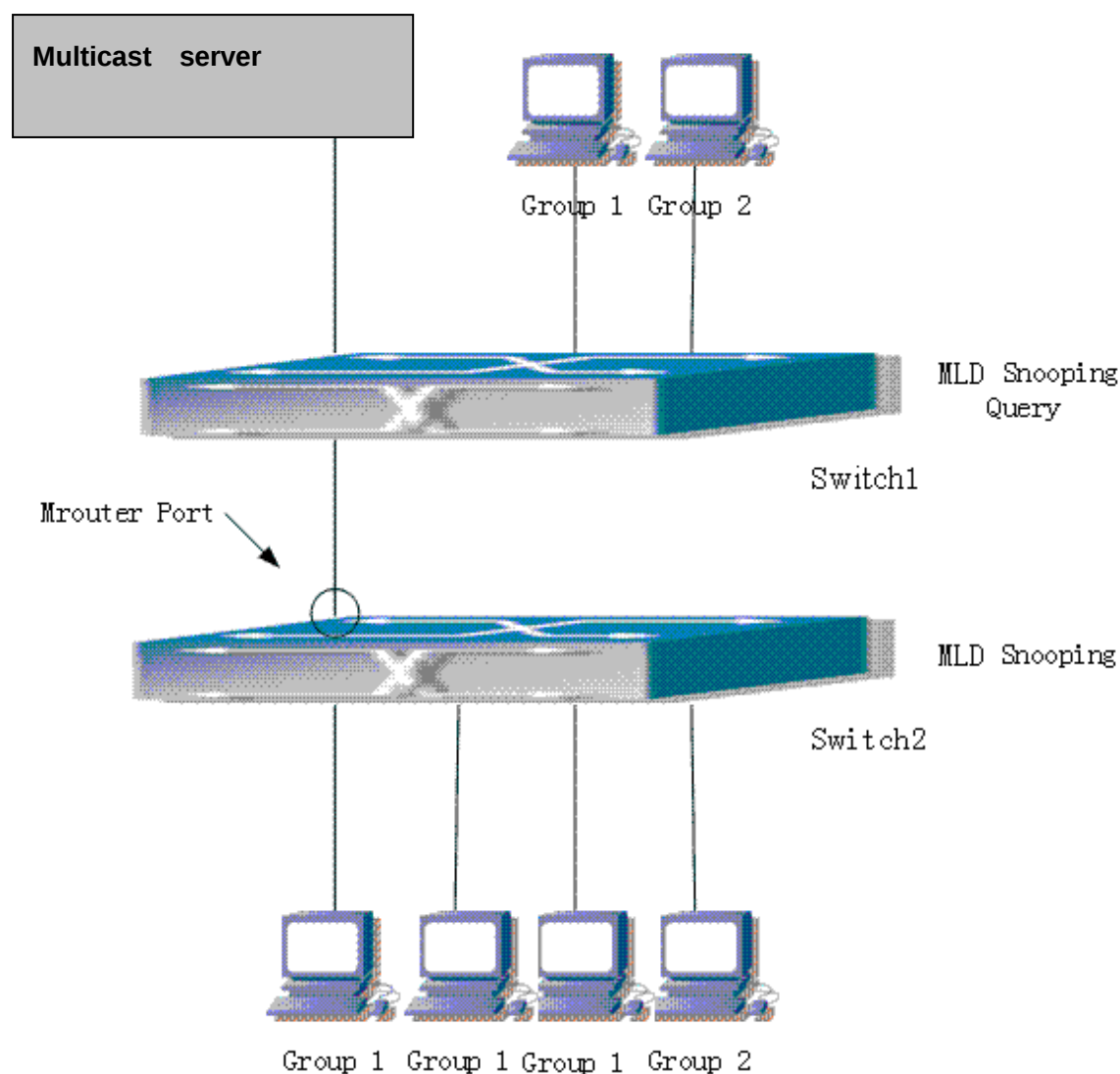


图 2-7 交换机作为 MLD Querier 功能图

switch B的配置与案例1中交换机相同，交换机switch 1取代案例1中的Multicast Router。假设其上配置VLAN 60包含端口1、2、10、12。端口1连接组播服务器，端口2连接switch2。为了定期发Query，需要打开全局下的MLD Snooping功能，同时需要执行mld snooping vlan 60 l2-general-querier，将VLAN 60设置成为二层普通查询者。

配置步骤如下：

```
switchA#config
```

```
switchA(config)#ipv6 mld snooping
```

```
switchA(config)#ipv6 mld snooping vlan 60
```

```
switchA(config)#ipv6 mld snooping vlan 60 l2-general-querier
```

```
switchB#config
```

```
switchB(config)#ipv6 mld snooping
```

```
switchB(config)#ipv6 mld snooping vlan 100
```

```
switchB(config)#ipv6 mld snooping vlan 100 mrouter interface ethernet 1/1
```

组播配置:

同案例1。

MLD Snooping侦听结果:

与案例1相似。

案例 3: 与三层组播协议混合运行

我们将案例 1 中的 SWITCH 替换为 ROUTER, 配置与原 SWITCH 配置相同, 组播配置与 MLD snooping 侦听结果与案例 1 相同。在 ROUTER 上全局启动 IPv6 三层组播(PIM-SM6), 同时在 VLAN 100 上启动 PIM SM6。(与上层组播路由器使用相同 PIM 模式)

配置步骤如下:

```
switch#config
switch(config)#ipv6 pim multicast-routing
switch(config)#interface vlan 100
switch(config-if-vlan100)#ipv6 pim sparse-mode
```

此时由于存在三层组播协议, MLD Snooping 不再下发表项, 只负责以下几件事情:

- ☞ 删除二层组播表项
- ☞ 向三层提供端口查询函数, 参数为 VLAN, S, G
- ☞ 当三层 MLD 关闭时, 重新下发二层组播表项

通过观察三层 IP6MC 表项, 发现三层组播出入表项仍然可以精确到端口, 保证了 MLD snooping 与三层组播协议的混合运行。

2.7.4 MLD Snooping排错帮助

在配置、使用MLD Snooping功能时, 可能会由于物理连接、配置错误等原因导致MLD Snooping未能正常运行。因此, 用户应注意以下要点:

- ☞ 应该保证物理连接的正确无误
- ☞ 保证全局配置模式下MLD Snooping打开 (使用ipv6 mld snooping)
- ☞ 保证全局配置模式下VLAN上配置MLD Snooping (使用ipv6 mld snooping vlan <vlan-id>)
- ☞ 确保同一网段内配置了一个VLAN作为二层普通查询者, 或者确保配置了静态mrouter
- ☞ 使用show ipv6 mld snooping vlan <vid>命令查看MLD Snooping信息是否正确

第3章 组播VLAN配置

3.1 组播VLAN介绍

基于当前的组播点播方式，当处于不同的VLAN 的用户点播时，每个VLAN 会在本VLAN 内复制一个组播流。这样的组播点播方式，浪费了大量的带宽。因此我们通过配置组播VLAN 的方式，将交换机的端口加入到组播VLAN 内，并在使能了IGMP Snooping /MLD Snooping功能以后，使不同VLAN 内的用户公用一个组播VLAN，组播流只是在一个组播VLAN 内进行传输，从而节省了带宽。由于组播VLAN 与用户VLAN 完全隔离，因此安全和带宽都得以保证。在配置了组播VLAN 以后就保证了组播信息流能够持续不断的发送到用户。

3.2 组播 VLAN配置任务

- 1. 启动组播 VLAN 功能
- 2. 配置 IGMP Snooping
- 3. 配置 MLD Snooping

1.启动组播 VLAN 功能

命令	解释
VLAN 配置模式	
multicast-vlan no multicast-vlan	配置一个 VLAN 启动组播 VLAN 功能。 no 操作关闭该 VLAN 的组播 VLAN 功能。
multicast-vlan association <vlan-list> no multicast-vlan association <vlan-list>	将一个组播 VLAN 与多个 VLAN 关联。 No 操作删除组播 VLAN 的关联 VLAN。
multicast-vlan association interface (ethernet port-channel) IFNAME no multicast-vlan association interface (ethernet port-channel) IFNAME	将特定端口关联到组播 VLAN 上，这样关联到组播 VLAN 的端口上都能收到组播流量； no 命令取消关联端口关联关系。
multicast-vlan mode {dynamic compatible} no multicast-vlan mode {dynamic compatible}	配置组播 vlan 的两种模式；本命令的 no 操作为取消组播 VLAN 的模式配置。

2.配置 IGMP Snooping

命令	解释
全局配置模式	
ip igmp snooping vlan <vlan-id> no ip igmp snooping vlan <vlan-id>	启动组播 VLAN 的 IGMP Snooping 功能。 No 操作关闭组播 VLAN 上的 IGMP Snooping。
ip igmp snooping no ip igmp snooping	启动 IGMP Snooping 功能。no 操作关闭全局 IGMP Snooping 功能。

3.配置 MLD Snooping

ipv6 mld snooping vlan <vlan-id> no ipv6 mld snooping vlan <vlan-id>	启动组播 VLAN 的 MLD Snooping 功能。No 操作关闭之组播 VLAN 上的 MLD Snooping。
ipv6 mld snooping no ipv6 mld snooping	启动 MLD Snooping 功能。no 操作关闭全局 MLD snooping 功能。

3.3 组播VLAN举例

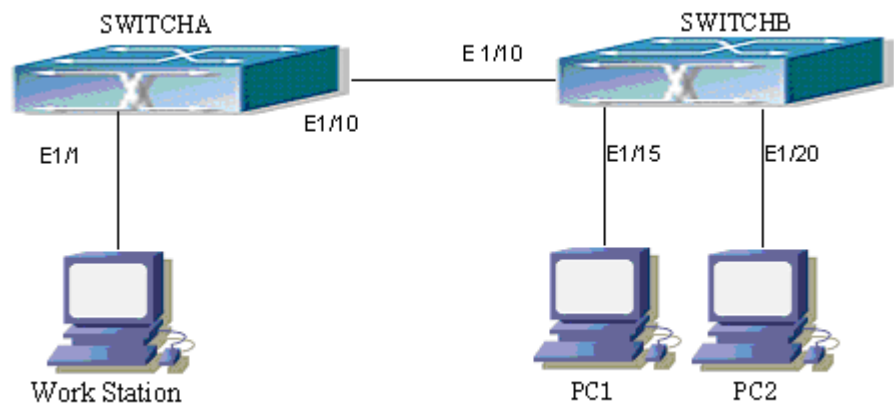


图 3-1 组播 VLAN 功能配置图

如图所示，组播服务器通过端口1/1与三层交换机switchA相连，端口1/1属于交换机的VLAN 10。三层交换机switchA通过端口1/10与二层交换机switchB相连，端口1/10配置为trunk模式。switchB上配置VLAN 100包含端口1/15，VLAN 101包含端口1/20。PC1和PC2分别连在端口1/15和1/20上。switchB通过端口1/10与交换机switchA相连，端口1/10配置为trunk模式。VLAN 20为组播VLAN。

通过配置组播VLAN，使PC1和PC2通过组播VLAN接收组播数据。

以下配置基于switchA的IP地址已经配置，并且设备连接正确的情况下进行配置。

配置步骤如下：

```
SwitchA#config
SwitchA(config)#vlan 10
SwitchA(Config-vlan10)#switchport interface ethernet 1/1
SwitchA(Config-vlan10)#exit
SwitchA(config)#interface vlan 10
SwitchA(Config-if-Vlan10)#ip pim dense-mode
SwitchA(Config-if-Vlan10)#exit
SwitchA(config)#vlan 20
SwitchA(config-vlan20)#exit
SwitchA(config)#interface vlan 20
SwitchA(Config-if-Vlan20)#ip pim dense-mode
SwitchA(Config-if-Vlan20)#exit
SwitchA(config)#ip pim multicast
SwitchA(config)#interface ethernet 1/10
SwitchA(Config-If-Ethernet1/10)#switchport mode trunk
```

```
SwitchB#config
SwitchB(config)#vlan 100
SwitchB(Config-vlan100)#switchport interface ethernet 1/15
SwitchB(Config-vlan100)#exit
SwitchB(config)#vlan 101
SwitchB(Config-vlan101)#switchport interface ethernet 1/20
SwitchB(Config-vlan101)#exit
SwitchB(config)#interface ethernet 1/10
SwitchB(Config-If-Ethernet1/10)#switchport mode trunk
SwitchB(Config-If-Ethernet1/10)#exit
SwitchB(config)#vlan 20
SwitchB(Config-vlan20)#multicast-vlan
SwitchB(Config-vlan20)#multicast-vlan association 100,101
SwitchB(Config-vlan20)#exit
SwitchB(config)#ip igmp snooping
SwitchB(config)#ip igmp snooping vlan 20
```

组播 VLAN 支持 IPV6 组播时,使用方法同 IPV4 原理相同,不同的只是与 MLD Snooping 配合使用,这里不再单独举例。