目 录

1 端口隔离

1.1 端口隔离简介

为了实现端口间的二层隔离，可以将不同的端口加入不同的 VLAN，但 VLAN 资源有限。采用端口隔离特性，用户只需要将端口加入到隔离组中，就可以实现隔离组内端口之间二层隔离，而不关心这些端口所属 VLAN，从而节省 VLAN 资源。

隔离组内的端口与未加入隔离组的端口之间二层流量双向互通。

1.2 端口隔离配置限制和指导

当二层聚合接口加入隔离组后，若在该二层聚合接口中新增 PEX 端口，则需要先将该二层聚合接口退出隔离组，然后重新加入隔离组。否则，该 PEX 端口不和隔离组中的其他端口二层隔离。有关 PEX 端口的介绍，请参见“虚拟化技术配置指导”中的“IRF3”。

VXLAN 组网中，如果 AC（以太网服务实例）关联的 VSI 配置了选择性泛洪的 MAC 地址（**selective-flooding mac-address**）并将 AC 所在端口加入同一隔离组，则 AC 可以将目的 MAC 地址匹配该泛洪 MAC 地址的数据帧转发给隔离组中的其他端口，不受隔离组影响。有关 VSI 选择性泛洪的 MAC 地址配置，请参见“VXLAN 配置指导”中“VXLAN/配置 VSI 泛洪抑制”。

VXLAN 组网中，如果同时配置 AC 链路为信任接口（**dhcp snooping trust**）并将 AC 所在端口加入同一隔离组，则 AC 可以将 DHCP 报文转发给隔离组中的其他端口，不受隔离组影响。有关 **dhcp snooping trust** 命令的配置，请参见“三层技术-IP 业务配置指导”中的“DHCP Snooping”。

1.3 配置隔离组

设备支持多个隔离组，用户可以手工配置。隔离组内可以加入的端口数量没有限制。

表1-1 配置隔离组

操作	命令	说明
进入系统视图	**system-view**	-
创建隔离组	**port-isolate group** *group-id*	缺省情况下，不存在隔离组
进入相应视图	• 进入二层以太网接口视图：**interface** *interface-type interface-number* • 进入二层聚合接口视图：**interface bridge-aggregation** *interface-number*	• 二层以太网接口视图下的配置只对当前端口生效 • 二层聚合接口视图下的配置对当前接口及其成员端口生效，若某成员端口配置失败，系统会跳过该端口继续配置其他成员端口，若二层聚合接口配置失败，则不会再配置成员端口
将端口加入到隔离组中	**port-isolate enable group** *group-id*	缺省情况下，当前端口不属于任何隔离组 一个端口最多只能加入一个隔离组

1.4 端口隔离显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后端口隔离的运行情况，通过查看显示信息验证配置的效果。

表1-2 端口隔离显示和维护

操作	命令
显示隔离组的信息	**display port-isolate group** [*group-id*]

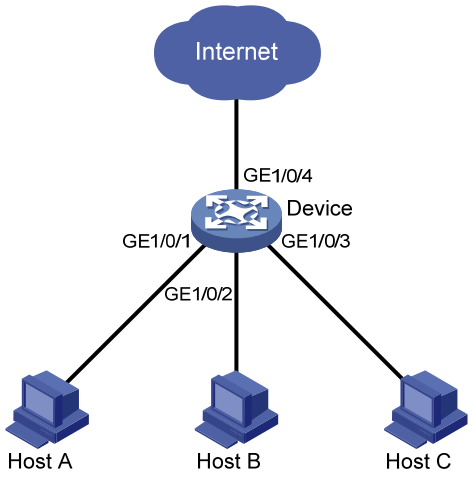
1.5 端口隔离典型配置举例

1. 组网需求

如 图 1-1 所示，小区用户Host A、Host B、Host C分别与Device的端口GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 相连，Device设备通过GigabitEthernet1/0/4 端口与外部网络相连。现需要实现小区用户Host A、Host B和Host C彼此之间二层报文不能互通，但可以和外部网络通信。

2. 组网图

图1-1 端口隔离组网图



3. 配置步骤

创建隔离组 2。

```
<Device> system-view
[Device] port-isolate group 2
[Device-port-isolate-group2] quit
```

将端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 加入隔离组 2。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-isolate enable group 2
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] port-isolate enable group 2
[Device-GigabitEthernet1/0/2] quit
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] port-isolate enable group 2
[Device-GigabitEthernet1/0/3] quit
```

4. 验证配置

显示隔离组 2 中的信息。

```
[Device] display port-isolate group 2
 Port isolation group information:
 Group ID: 2
 Group members:
   GigabitEthernet1/0/1     GigabitEthernet1/0/2     GigabitEthernet1/0/3
 Community VLAN ID: None
```

以上信息显示 Device 上的端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 已经加入隔离组 2，从而实现二层隔离，Host A、Host B 和 Host C 彼此之间不能 ping 通。