PVLAN 技术白皮书

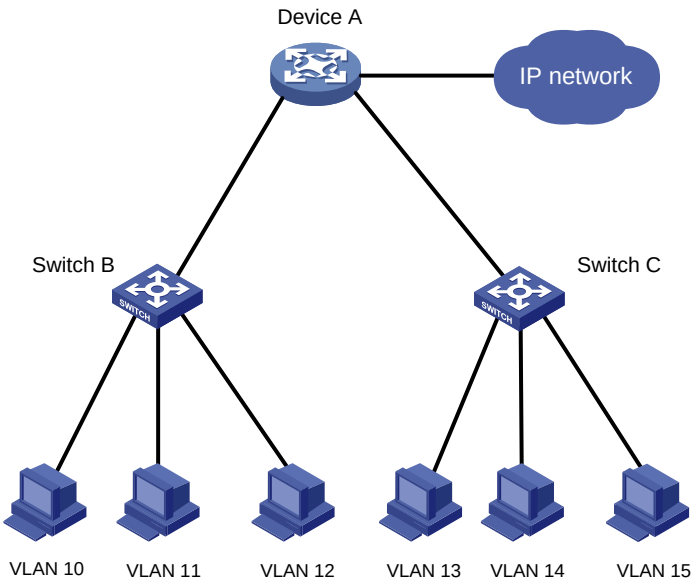
目 录

1 PVLAN 概述

1.1 PVLAN产生背景

以太网的快速发展对传统 VLAN 网络提出了更高的要求，基于用户安全和管理计费等方面的考虑，一般要求接入用户二层互相隔离。VLAN 是天然的隔离手段，很自然的想法是每个用户一个 VLAN。如图 1 所示，Switch B 和 Switch C 上分别接入三个用户，如果给每个用户划分一个 VLAN，则需要占用 Device A 上的六个 VLAN 资源。

图1 传统 VLAN 网络



根据 IEEE 802.1Q 协议规定，设备最大可使用 VLAN 资源为 4094 个。对于核心层设备来说，如果每个用户一个 VLAN，4094 个 VLAN 远远不够，而且在一般的交换设备中，通常是采用一个 VLAN 对应一个 VLAN 接口的方式来实现 VLAN 之间的互通，这将耗费大量的 IP 地址、增加部署成本与日常维护管理难度。为了解决上述问题，PVLAN（Private VLAN，私有 VLAN）技术应运而生。

1.2 PVLAN技术优点

- 节省 VLAN 及 IP 资源：

  PVLAN 采用两层 VLAN 隔离技术，即分为上行 Primary VLAN 和下行 Secondary VLAN。上行设备只可见 Primary VLAN，而不必关心 Private VLAN 中的 Secondary VLAN，从而大大节省了上行设备的 VLAN 资源。

  PVLAN 支持 L3 域功能，对下行不同的 Secondary VLAN，均可使用 Primary VLAN 接口作为网关，并且支持不同 Secondary VLAN 之间的三层互通，有效地节省了紧缺的 IP 资源。
- 安全性：

  下行 Secondary VLAN 在配置为 Isolated VLAN 后，具备隔离功能，同一 Secondary VLAN 内各端口二层隔离，增强了安全性。
- 高性能：

PVLAN 转发采用 MAC 地址同步技术，同时 PVLAN L3 域的广播报文在 Primary VLAN 内通信时由芯片完成发送，具有较高的转发性能。

2 PVLAN 技术实现

2.1 PVLAN相关术语

- Private VLAN：由一组 VLAN 集构成，包括 1 个 Primary VLAN 和其对应的 Secondary VLAN。
- Primary VLAN：上行设备感知的用户 VLAN，它并不是用户的真正 VLAN。
- Secondary VLAN：用户真正属于的 VLAN。Secondary VLAN 有两种类型：Community VLAN 和 Isolated VLAN。同一 Community VLAN 内的下行端口（又称为 Community port）可以互通，同一 Isolated VLAN 内的下行端口(又称为 Isolated port)相互隔离。缺省情况下，Secondary VLAN 为 Community VLAN。
- PVLAN L3 域：通过在 Primary VLAN 接口上指定三层互通的 Secondary VLAN，配置 Primary VLAN 接口的 IP 地址并开启本地代理 ARP（Address Resolution Protocol，地址解析协议）/ND（Neighbor Discovery，邻居发现）功能可以建立 PVLAN L3 域。其中三层互通的 Secondary VLAN 被认为加入了该 PVLAN L3 域，这些 Secondary VLAN 共用 Primary VLAN 接口作为网关，大大节省了 IP 资源。

2.2 PVLAN技术原理

为了在上行设备上屏蔽 Secondary VLAN 信息，达到节省 VLAN 资源的目的，需要 PVLAN 实现：

- 来自不同 Secondary VLAN 的报文，能够通过上行端口发送给上行设备，而且不能携带 Secondary VLAN 信息。
- 来自 Primary VLAN 的报文，能够通过下行端口发送给用户，而且不能携带 Primay VLAN 信息。

PVLAN 技术中，上下行接口可以采用不同的 PVLAN 工作模式，在出方向剥离 VLAN Tag 或替换 VLAN Tag，完成屏蔽 VLAN 的功能。其次，PVLAN 采用配置同步以及 MAC 地址同步技术，简化了用户的配置，提高了报文转发的效率以及安全性。同时，PVLAN 支持 L3 域，对于加入 PVLAN L3 域的 Secondary VLAN，可通过 Primary VLAN 接口进行三层互通。

2.2.1 PVLAN 端口工作模式

PVLAN 为端口提供了 Host、Trunk secondary、Promiscuous 和 Trunk promiscuous 四种工作模式：

- Host 工作模式：工作在 Host 模式的端口用于与用户相连，负责和终端通信，属于下行端口。对于 Host 模式的端口，需确保其缺省 VLAN 为 Secondary VLAN，否则该端口无法转发来自 Primary VLAN 的报文。Host 模式适用于只有一个 Secondary VLAN 通过下行端口的情况，该模式下 Secondary VLAN 不带 Tag 通过下行端口。
- Trunk secondary 工作模式：工作在 Trunk secondary 模式的端口用于和下行设备相连，属于下行端口。报文携带的 Primary VLAN ID 在端口出方向上会替换为对应 Secondary VLAN ID，从而对于下行设备屏蔽了 Primary VLAN。Trunk secondary 模式的端口，对于同一个 Primary

VLAN 只能加入一个 Secondary VLAN，但可加入多个不同 Primary VLAN 对应的 Secondary VLAN。Trunk secondary 模式适用于需要多个 Secondary VLAN 通过下行端口的情况，该模式下多个 Secondary VLAN 携带 Tag 通过下行端口。

- Promiscuous 工作模式：工作在 Promiscuous 模式的端口用于和上行设备相连，负责和上行设备通信，属于上行端口。Promiscuous 模式的端口，需确保其缺省 VLAN 为 Primary VLAN，否则该端口无法转发来自 Secondary VLAN 的报文。Promiscuous 适用于只有一个 Primary VLAN 通过上行端口的情况，该模式下 Primary VLAN 不带 Tag 通过上行端口。
- Trunk pomiscuous 工作模式：工作在 Trunk promiscuous 模式的端口用于和上行设备相连，属于上行端口。报文携带的 Secondary VLAN ID 在端口出方向上会替换为对应 Primary VLAN ID，从而对于上行设备屏蔽了 Secondary VLAN。Trunk promiscuous 模式适用于多个 Primary VLAN 携带 Tag 通过上行端口。

其中，Promiscuous 工作模式和 Trunk promiscuous 工作模式应用于上行端口；Host 工作模式和 Trunk secondary 工作模式应用于下行端口，与 Isolated VLAN 一起应用时具有隔离功能。通过这四种工作模式，可以对 PVLAN 的应用进行灵活组网，如图 2 和图 3 所示。

图2 Promiscuous&Host 工作模式应用示意图

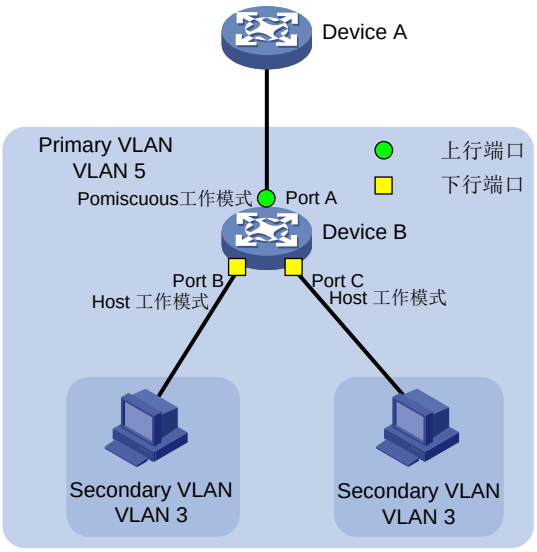
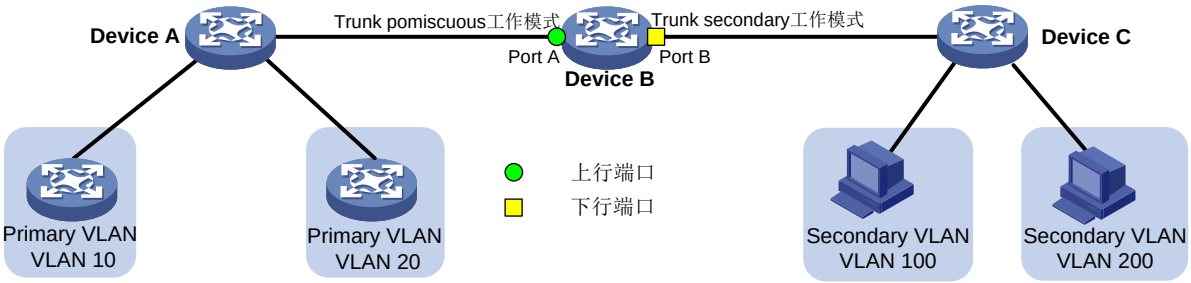


图3 Trunk pomiscuous&Trunk secondary 工作模式应用示意图

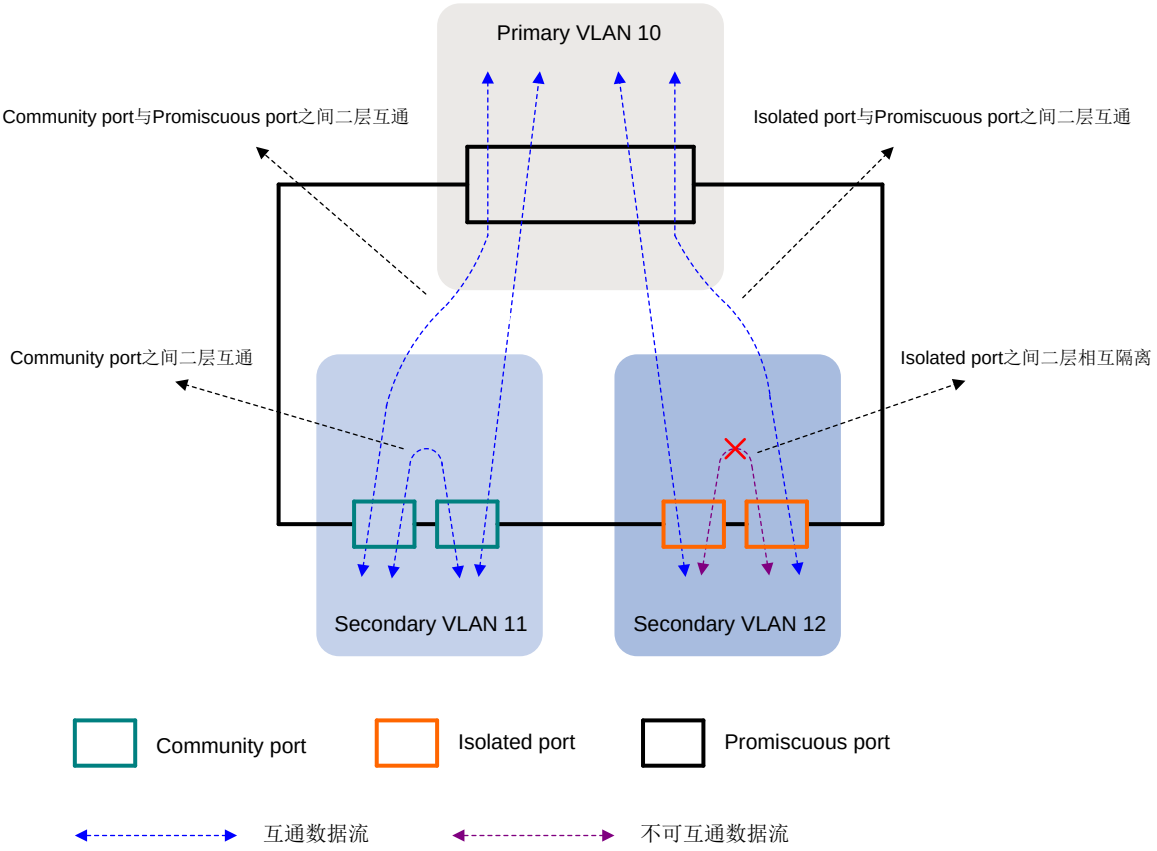


2.2.2 PVLAN 端口间的互通

如图 4 所示，各工作模式端口间的互通关系为（假设上行端口工作在 Promiscuous 模式，Trunk promiscuous 模式的上行端口与此相同）：

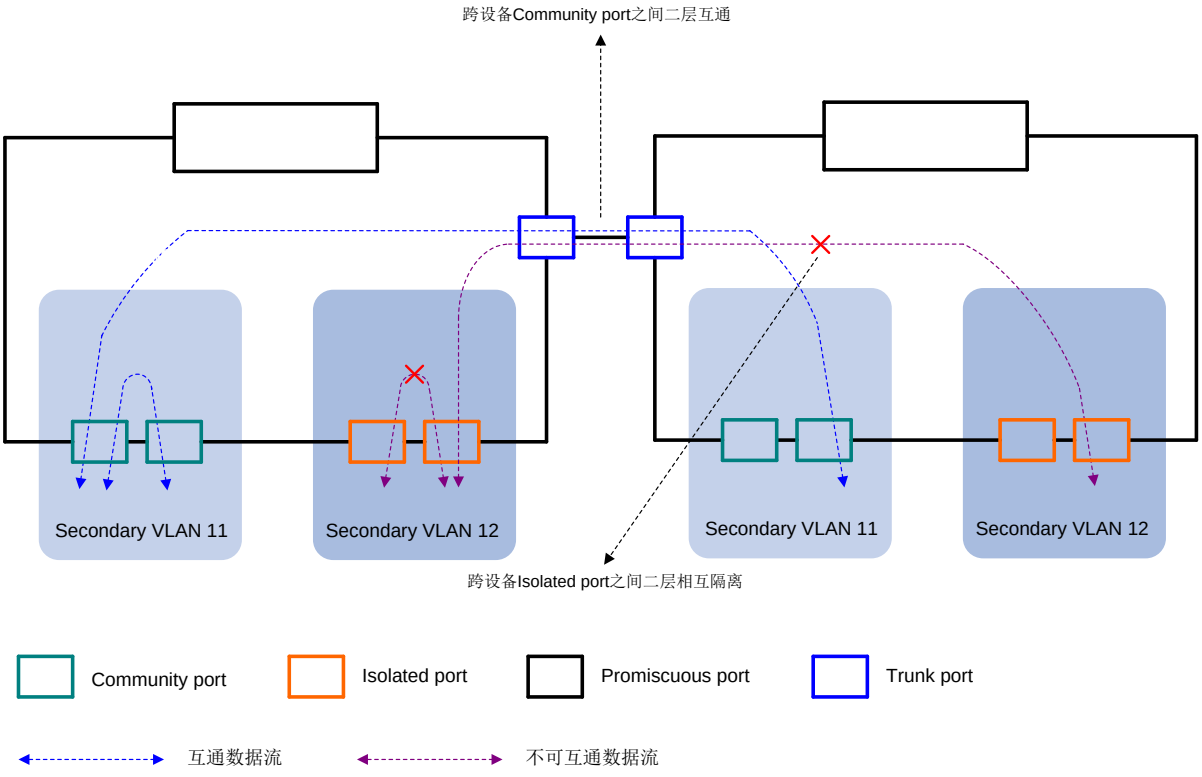
- Community port 与 Promiscuous port 之间可以互通。
- Community port 之间可以互通。
- Isolated port 与 Promiscuous port 之间可以互通。
- Isolated port 之间不能互通。

图4 PVLAN 各工作模式端口间的互通关系



PVLAN 除了支持本设备内下行端口隔离之外，同样也支持 Isolated VLAN 的跨设备隔离。对于 Isolated VLAN 的跨设备隔离，要求报文可以携带 Isolated VLAN Tag 发送到其它设备上，借助 Trunk 口（或 Hybrid 口），可以完成跨设备的隔离。如图 5 所示，对于 Device A 到 Device B 的流量，Community port 之间能够互通，Isolated port 之间不能互通。

图5 PVLAN 跨设备隔离



2.2.3 PVLAN 配置同步

PVLAN 配置同步技术能够对 Primary VLAN 和 Secondary VLAN 所包含的端口进行自动同步，在 Primary VLAN 下有大量 Secondary VLAN 的环境中，极大地简化了用户对 PVLAN 功能的部署过程。

PVLAN 配置同步的触发需要同时满足三个条件：配置开启 Primary VLAN、Primary VLAN 与 Secondary VLAN 建立映射关系，以及端口配置 PVLAN 工作模式。三个条件的配置无先后依赖关系。配置同步后，端口上的如下两方面的配置将会发生变化：端口类型，端口加入 Primary VLAN 与 Secondary VLAN。

(1) 端口类型：对于 Access 类型的接口，切换为 Hybrid 类型；对于 Trunk/Hybrid 类型的接口保持原接口类型不变。

(2) 端口加入 Primary VLAN 与 Secondary VLAN：若端口此前存在以 Tagged/Untagged 方式加入某些 VLAN 的配置，则在保持原有配置的基础上，端口会以下面原则加入其它的 VLAN：

- 对于 Host 工作模式的下行端口，以 Untagged 方式加入 Primary VLAN。
- 对于 Trunk secondary 工作模式的下行端口，以 Tagged 方式加入 Primary VLAN 和 Secondary VLAN。
- 对于 Promiscuous 工作模式的上行端口，以 Untagged 方式加入 Secondary VLAN。
- 对于 Trunk promiscuous 工作模式的上行端口，以 Tagged 方式加入 Primary VLAN 和 Secondary VLAN。

如图 6 所示的组网中，端口的相关属性如表 1 所示。

在 Device A 上做如下配置：

- 配置 VLAN 10 为 Primary VLAN，VLAN 201、301 为其对应的 Secondary VLAN。
- 配置 GigabitEthernet1/0/1 在 VLAN 10 中工作在 Promiscuous 模式，GigabitEthernet1/0/2、GigabitEthernet1/0/3 在 VLAN 301、201 中工作在 Host 模式。

在 Device B 上做如下配置：

- 配置 VLAN 10 为 Primary VLAN，VLAN 201 为其对应的 Secondary VLAN。
- 配置 VLAN 20 为 Primary VLAN，VLAN 401 为其对应的 Secondary VLAN。
- 配置 GigabitEthernet1/0/1 在 VLAN 10、20 中工作在 Trunk promiscuous 模式，GigabitEthernet1/0/2 在 VLAN 201 中工作在 Host 模式，GigabitEthernet1/0/3 在 VLAN 201、401 中工作在 Trunk secondary 模式。

配置同步后，端口的相关属性发生了改变，具体信息如图 6 表 2 所示。

图6 PVLAN 配置同步组网图

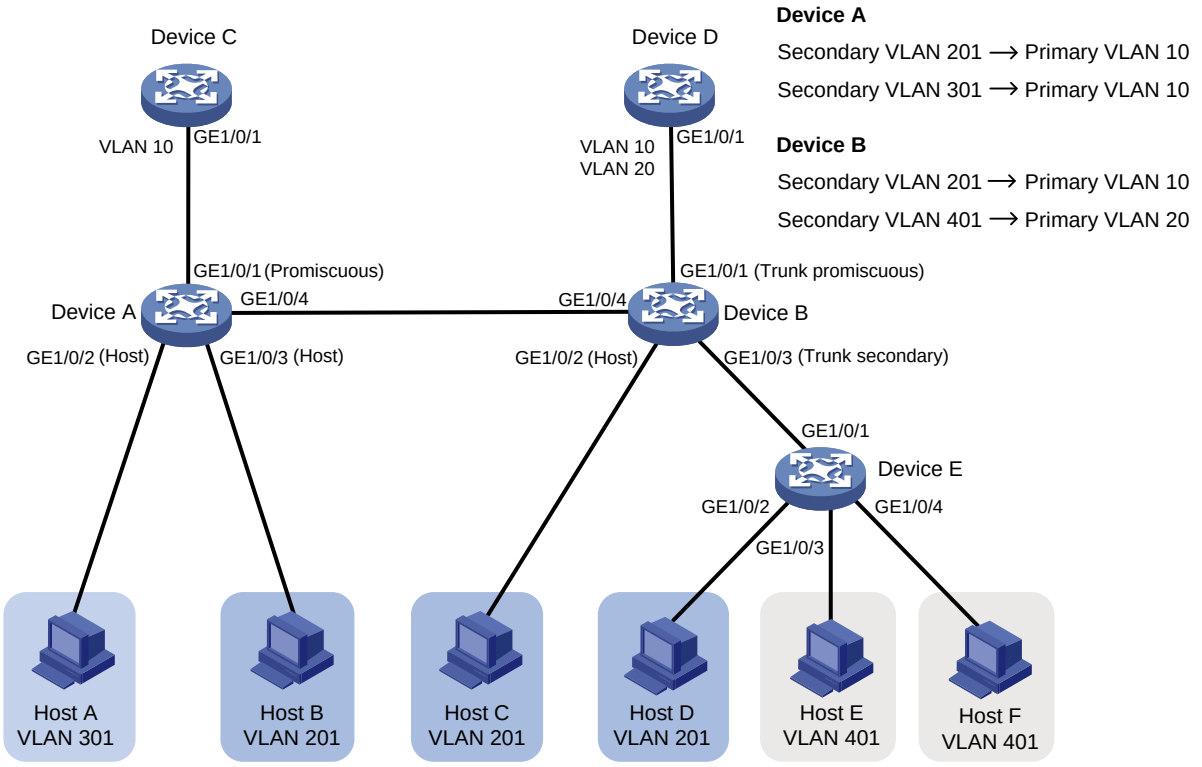


表1 配置同步前端口的相关属性

设备	端口	类型	工作模式	端口缺省 VLAN	允许通过的 VLAN
Device A	GigabitEthernet1/0/1	Access	N/A	10	只允许VLAN 10的报文通过
Device A	GigabitEthernet1/0/2	Access	N/A	301	只允许VLAN 301的报文通过
Device A	GigabitEthernet1/0/3	Access	N/A	201	只允许VLAN 201的报文通过
Device B	GigabitEthernet1/0/1	Access	N/A	1	只允许VLAN 1的报文通过

设备	端口	类型	工作模式	端口缺省 VLAN	允许通过的 VLAN
Device B	GigabitEthernet1/0/2	Access	N/A	201	只允许VLAN 201的报文通过
Device B	GigabitEthernet1/0/3	Access	N/A	1	只允许VLAN 1的报文通过

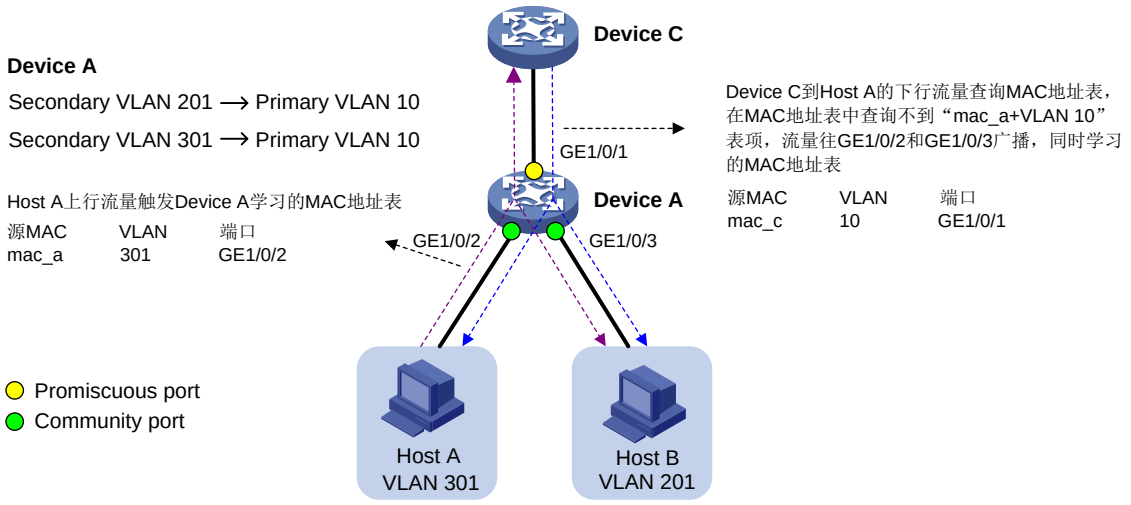
表2 配置同步后端口的相关属性

设备	端口	类型	工作模式	端口缺省 VLAN	允许通过的 VLAN
Device A	GigabitEthernet1/0/1	Hybrid	Promiscuous (VLAN 10)	10	允许VLAN 10、201、301的报文通过
Device A	GigabitEthernet1/0/2	Hybrid	Host	301	允许VLAN 10、301的报文通过
Device A	GigabitEthernet1/0/3	Hybrid	Host	201	允许VLAN 10、201的报文通过
Device B	GigabitEthernet1/0/1	Hybrid	Trunk promiscuous (VLAN 10, 20)	1	允许VLAN 1、10、201、20、401的报文通过
Device B	GigabitEthernet1/0/2	Hybrid	Host	201	允许VLAN10、201的报文通过
Device B	GigabitEthernet1/0/3	Hybrid	Trunk secondary (VLAN 201, 401)	1	允许VLAN 1、10、201、20、401的报文通过

2.2.4 MAC 地址同步

PVLAN 不进行 MAC 地址同步时的转发流程如图 7 所示。通过 MAC 地址学习，Device A 会生成并维护一张 MAC 地址表（如表 3 所示）。如果 Device C 给 Host A 发送报文（源 MAC 为 mac_c，目的 MAC 为 mac_a）；Device A 会给报文添加 Tag，VLAN ID 为 10（即端口的缺省 VLAN ID）；然后以“mac_a+VLAN 10”为条件去查询 MAC 地址表。由于找不到相应的表项，该报文会在 VLAN 10 内广播，并最终从 GigabitEthernet1/0/2、GigabitEthernet1/0/3 发送出去（如图 7 中蓝色箭头所示）。

图7 PVLAN 无 MAC 同步转发流程图



在如图 8 示组网中，Device A 上的 MAC 地址表如表 3 所示。因此，每次上行和下行的报文都需要广播才能到达目的地。当 Secondary VLAN 和 Primary VLAN 包含的端口较多时，这样的处理方式会占用大量的带宽资源，形成大量的广播报文，同时也存在安全问题（如易被截获和侦听）。通过 MAC 地址同步机制可以解决这个问题。

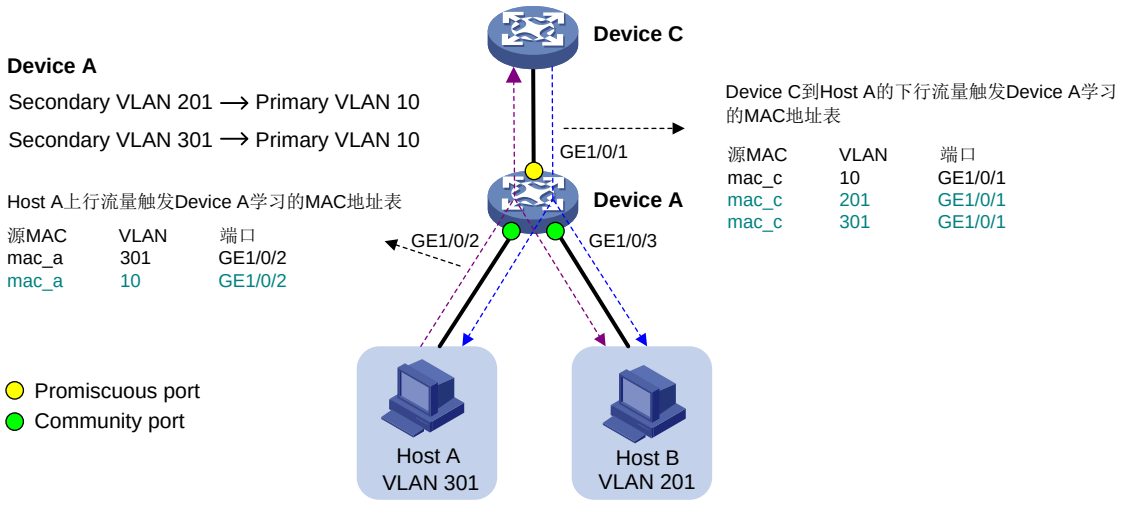
表3 同步前的 MAC 地址表

源 MAC 地址	VLAN	出端口
mac_c	10	GigabitEthernet1/0/1
mac_a	301	GigabitEthernet1/0/2
mac_b	201	GigabitEthernet1/0/3

MAC 地址同步原理如下：

- Secondary VLAN 到 Primary VLAN 的同步，即下行端口在 Secondary VLAN 内学习到的动态 MAC 地址都同步到 Primary VLAN 内。
- Primary VLAN 到 Secondary VLAN 的同步，即上行端口在 Primary VLAN 学习到的动态 MAC 地址同步到所有的 Secondary VLAN 内。

图8 PVLAN MAC 地址同步转发流程图



在如图 8 所示的组网中，Device A 上 MAC 地址同步后生成的 MAC 地址表如表 4 所示。

表4 同步后的 MAC 地址表

源 MAC 地址	VLAN	出端口
mac_c	10	GigabitEthernet1/0/1
mac_c	201	GigabitEthernet1/0/1
mac_c	301	GigabitEthernet1/0/1
mac_a	301	GigabitEthernet1/0/2
mac_a	10	GigabitEthernet1/0/2
mac_b	201	GigabitEthernet1/0/3
mac_b	10	GigabitEthernet1/0/3

当 Primary VLAN 下面配置了很多 Secondary VLAN，MAC 地址同步后，将导致 MAC 地址表过于庞大，进而影响设备的转发性能。同时考虑到用户的下行流量要远远大于上行流量，下行流量需要进行单播，上行流量可以进行广播。所以，Secondary VLAN 到 Primary VLAN 的同步所有产品均支持，而 Primary VLAN 到 Secondary VLAN 的同步部分产品不支持。

以上为 Promiscuous port 和 Community port 之间的通信；Trunk promiscuous port 和 Community port 之间的 MAC 通信与此相同。对于 Promiscuous port 或 Trunk promiscuous port 与 Isolated port 之间的通信，MAC 地址同步机制类似，所不同的是同一个 Secondary VLAN 下的 Isolated port 之间二层相互隔离。

2.2.5 PVLAN L3 域

加入 PVLAN L3 域的 Secondary VLAN，通过 Primary VLAN 的 VLAN 接口进行三层互通，Secondary VLAN 本身不允许再创建自己的 VLAN 接口。未加入 PVLAN L3 域的 Secondary VLAN，可以创建自己的 VLAN 接口进行三层通信，组网上更为灵活。

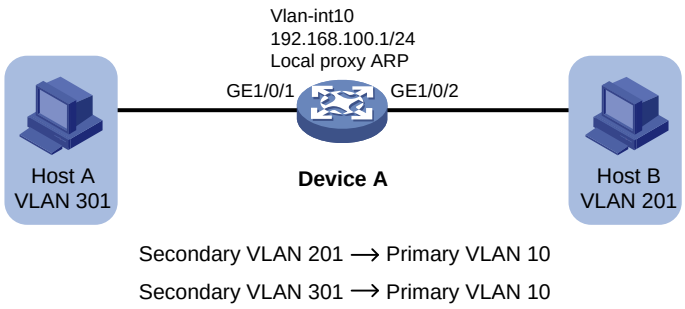
如图 9 所示，Device A 支持 PVLAN L3，在 Device A 的 Primary VLAN 接口上配置本地代理 ARP/ND 功能，实现 Secondary VLAN 之间的互通。通信的过程如下：

(1) VLAN 接口 10 上配置了本地代理 ARP 功能，VLAN 接口 10 接收到 Host A 发送的 ARP 请求后，会用自己的 MAC 地址代理回应 ARP 请求。

(2) VLAN 接口 10 以自己为源向除 GigabitEthernet1/0/1 以外的接口发送 ARP 请求获取 Host B 的 MAC 地址，接收到 Host B 的应答后，ARP 表项建立完成。

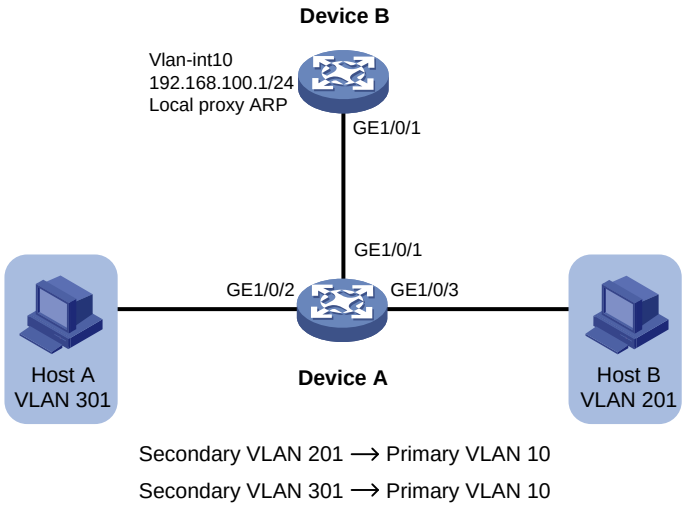
(3) Host A 与 Host B 互相通信时均认为对方的 MAC 地址为 VLAN 接口 10 的 MAC 地址。

图9 本地设备配置本地代理 ARP/ND 功能实现 Secondary VLAN 之间三层互通



如图 10 所示，PVLAN 配置在不支持 PVLAN L3 域的 Device A 上，若要实现不同 Secondary VLAN 之间的互通，只能依靠在上层设备 Device B 上配置本地代理 ARP/ND 功能来实现。通信流程与本地设备配置本地代理 ARP/ND 功能流程一致，但这样会增加上层设备的负担。

图10 上层设备配置本地代理 ARP/ND 功能实现 Secondary VLAN 之间互通



2.3 PVLAN应用限制

- VLAN 1 不能进行 PVLAN 相关配置。
- PVLAN 配置同步包括端口加入 VLAN 以及将 Access 端口的链路类型改为 Hybrid 类型。对于端口缺省 VLAN 配置和端口已有的 VLAN Tagged/Untagged 属性，不包含在易用性范围内，

要求用户手工保证配置正确。执行 undo 命令使配置不再满足 PVLAN 配置同步条件时，相关端口由于 PVLAN 配置同步触发的配置修改不会恢复为原本的配置。

- PVLAN 与二层组播组合使用时，在 Primary VLAN 上进行的二层组播配置，会同步到与其建立映射的 Secondary VLAN 上，因此不建议在 Secondary VLAN 上配置组播协议。
- 当 PVLAN 设备与 PVST（Per-VLAN Spanning Tree，每 VLAN 生成树）设备进行对接时，要求与上行的 PVST 设备连接的端口工作在 Trunk promiscuous 模式，与下行的 PVST 设备连接的端口工作在 Trunk secondary 模式，并且要求 PVST 设备上与 PVLAN 设备相连端口的链路类型为 Trunk 类型，否则将触发端口类型不一致保护或者 PVID 不一致保护。

3 PVLAN 组网应用

3.1.1 PVLAN 二层应用

基于 PVLAN 二层节省 VLAN 以及支持 Secondary VLAN 隔离的特点，用户可以用较少的 VLAN 资源完成二层组网。

如图 11 所示，要求所有 Host 可以与 Server 进行通信。其中，Host A 和 Host D 之间相互隔离，其它在同一 Secondary VLAN 下的 Host 之间可以二层互通。

在 Device A 上进行如下配置：

- 配置 Primary VLAN 10，Isolated VLAN 301 和 Community VLAN 201 为其对应的 Secondary VLAN。
- 配置 GigabitEthernet1/0/1 在 Isolated VLAN 301 下工作在 Host 模式。
- 配置 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 在 Community VLAN 201 下工作在 Host 模式。
- 配置 GigabitEthernet1/0/4 为 Trunk 口，加入 Primary VLAN 10、Isolated VLAN 301 和 Community VLAN 201，以支持在 Isolated VLAN 301 中的 Host A 与 Host D 的隔离以及其它在同一 Secondary VLAN 下的 Host 之间的二层互通。
- 配置 GigabitEthernet1/0/5 在 Primary VLAN 10 中工作在 Promiscuous 模式，与上游的 Device D 相连。

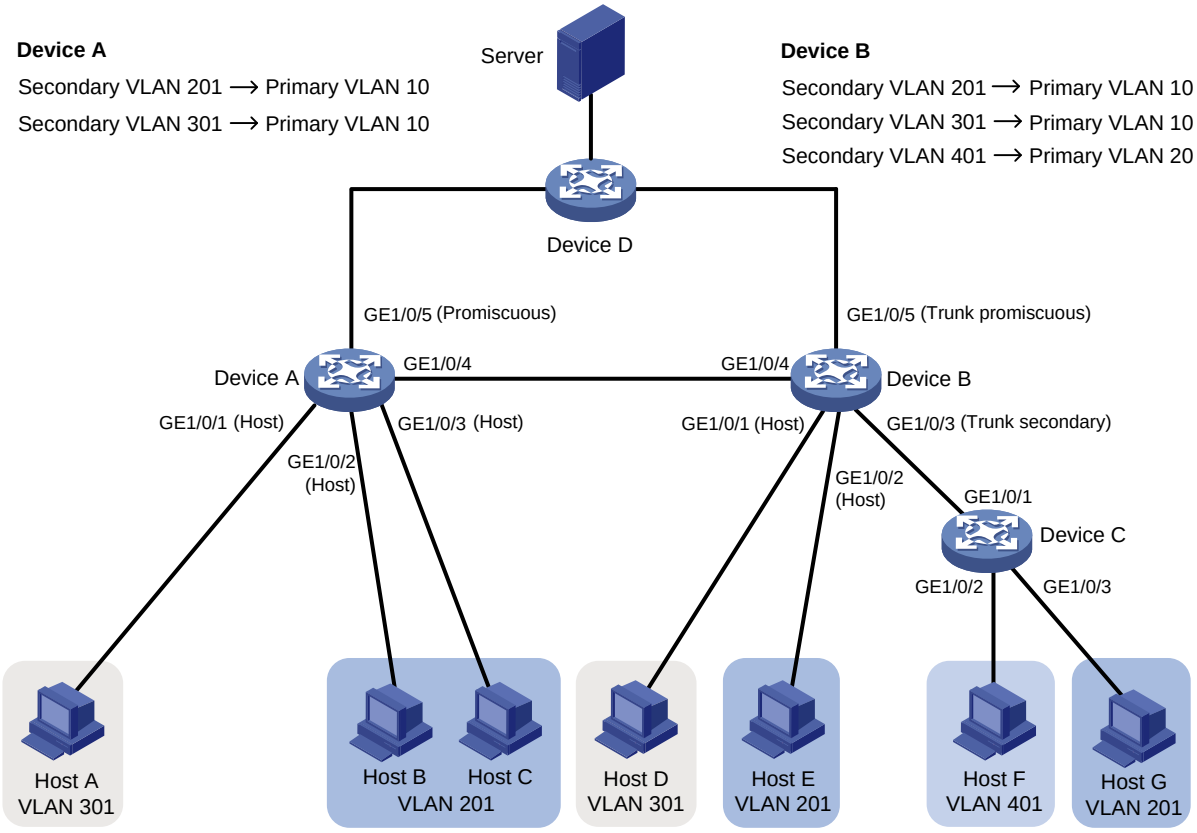
在 Device B 上进行如下配置：

- 配置 Primary VLAN 10，Isolated VLAN 301 和 Community VLAN 201 为其对应的 Secondary VLAN；配置 Primary VLAN 20，Community VLAN 401 为其对应的 Secondary VLAN。
- GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/4 的配置与 Device A 上的配置一致。
- 配置 GigabitEthernet1/0/3 在 Secondary VLAN 201、401 中工作在 Trunk secondary 模式，与下游的 Device C 相连。
- 配置 GigabitEthernet1/0/5 在 Primary VLAN 10、20 中工作在 Trunk promiscuous 模式，与上游的 Device D 相连。

在 Device C 上进行如下配置：

- 配置 GigabitEthernet1/0/1 为 Trunk 口，加入 VLAN 201、401。
- 配置 Access 口 GigabitEthernet1/0/2、GigabitEthernet1/0/3 的 PVID 分别为 401、201。

图11 PVLAN 二层典型组网图



组网配置完成后：

- Host B 与 Server 的通信：从 Server 到 Host B 的下行流量，通过 Device A 的 GigabitEthernet1/0/5 进入，为其添加 VLAN Tag 10，通过 GigabitEthernet1/0/2 剥离其 VLAN Tag 后到达 Host B。从 Host B 到 Server 的上行流量，通过 Device A 的 GigabitEthernet1/0/2 进入，为其添加 VLAN Tag 201，通过 Device A 的 GigabitEthernet1/0/5 剥离其 VLAN Tag 后到达 Server 的接入设备 Device D。
- Host A 与 Server 的通信：和 Host B 与 Server 的通信类似。需要指出的是，从 Host A 发出的广播报文（VLAN Tag 为 Isolated VLAN 301），可以到达 Server，但无法到达 Host D，原因是报文到达 Device B 的 GigabitEthernet1/0/1 时，由于该端口属于 Isolated VLAN，报文无法在 GigabitEthernet1/0/1 口进行转发。
- Host F 与 Server 的通信：从 Host F 到 Server 的上行流量，通过 Device C 的 GigabitEthernet1/0/2 进入，封装 VLAN 401 的 Tag，并在 GigabitEthernet1/0/1 携带 VLAN 401 的 Tag 发送，报文到达 Device B 后，在 VLAN 401 内进行转发，在 Device B 的 GigabitEthernet1/0/5 替换其 VLAN Tag 为 VLAN 20 后进行发送，到达 Server 的接入设备 Device D。

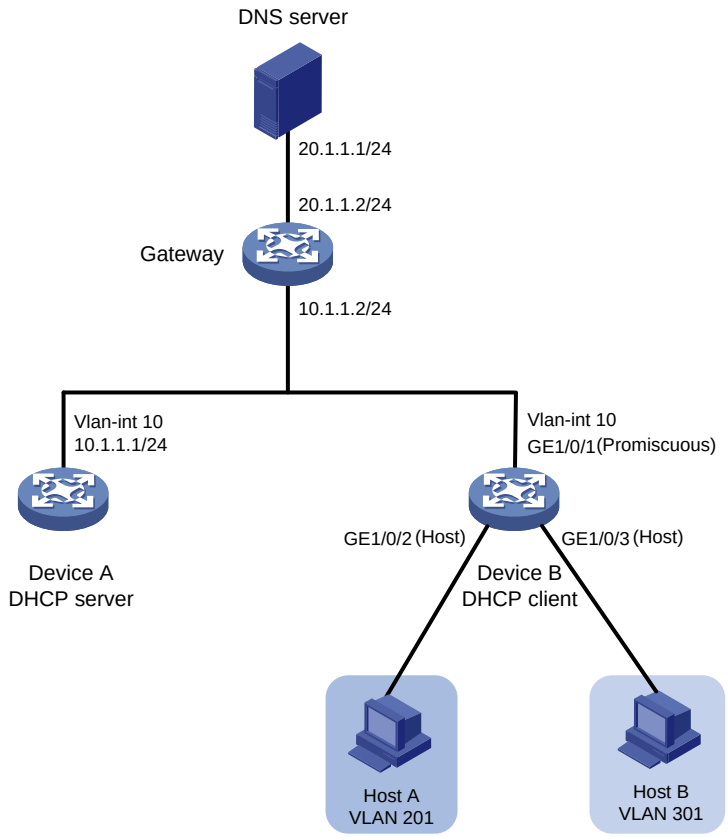
3.1.2 PVLAN 三层应用

通过对 PVLAN L3 域功能的支持，可以使 PVLAN 在三层领域有更多的应用。

1. PVLAN 与 DHCP 组合应用

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）用来为网络设备动态分配 IP 地址等网络配置参数。PVLAN 功能可以通过 DHCP 为 Primary VLAN 10 的 VLAN 接口和 Secondary VLAN 中的 Host 申请 IP 地址以及其他配置信息，以便 Secondary VLAN 之间以及 Secondary VLAN 与外部进行互通，如图 12 所示。

图12 PVLAN 与 DHCP 组网图



在 Device B 上进行如下配置：

- 配置 VLAN 10 为 Primary VLAN，VLAN 201、301 为其对应的 Secondary VLAN。
- 配置 Primary VLAN 10 下的 Secondary VLAN 201、301 三层互通，同时在 VLAN 接口 10 上开启本地代理 ARP 功能。
- 配置 GigabitEthernet1/0/1 在 VLAN 10 中工作在 Promiscuous 模式。
- 配置 VLAN 接口 10 通过 DHCP 协议从 DHCP 服务器获取 IP 地址、DNS（Domain Name System，域名系统）服务器地址和静态路由信息。

在 Device A 上进行如下配置：

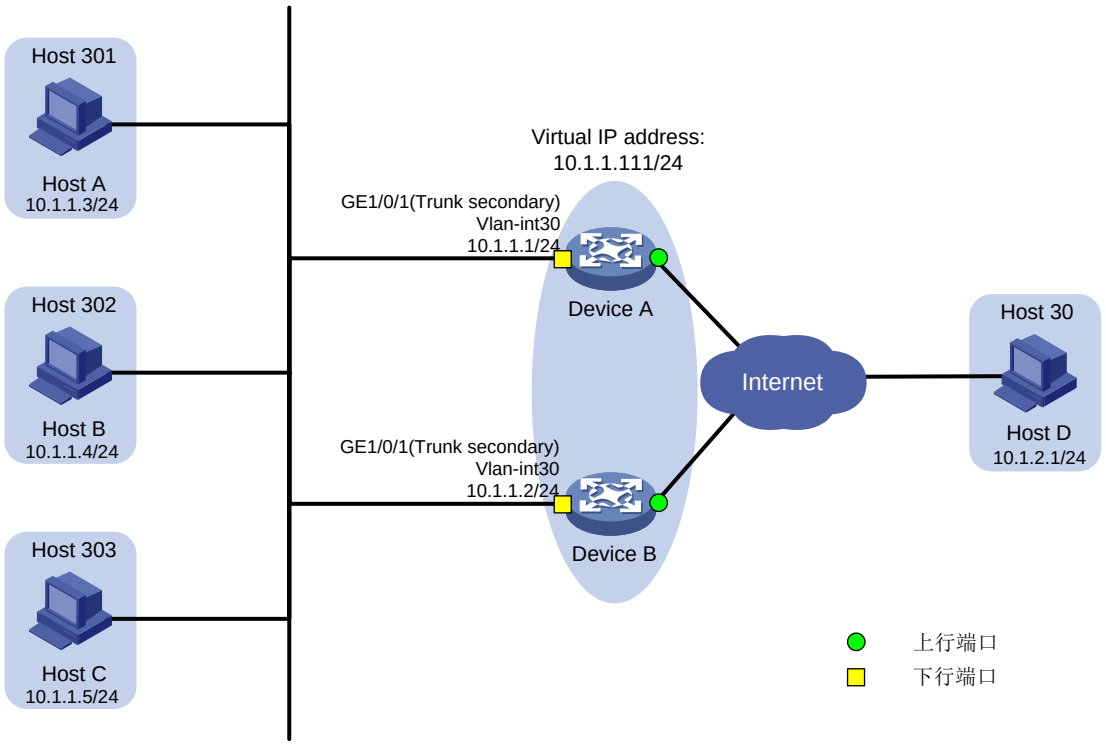
- 配置 VLAN 接口 10 工作在 DHCP 服务器模式。
- 配置 DHCP 地址池，用来为 10.1.1.0/24 网段内的客户端分配 IP 地址和网络配置参数。其中 DNS 服务器地址为 20.1.1.1/24，网关的地址为 10.1.1.2/24。

通过上面的组网，Host A 和 Host B 可以通过 Primary VLAN 10 的 VLAN 接口申请到 IP 地址和其它配置信息。

2. PVLAN 与 VRRP 组合应用

如图 13 所示，Host A、Host B 和 Host C 需要访问 Internet 上的 Host D。

图13 PVLAN 与 VRRP 组网图



采用 VRRP（Virtual Router Redundancy Protocol，虚拟路由器冗余协议）技术，将 Device A 和 Device B 加入备份组，提高组网的可靠性。当 Device A 正常工作时，Host A 发送给 Host D 的报文通过 Device A 转发；当 Device A 出现故障时，Host A 发送给 Host D 的报文通过 Device B 转发。当Device A故障恢复后，Device A会抢占成为Master，Host A发送给Host D的报文仍然通过Device A 转发。

采用 PVLAN L3 域技术，Device A 和 Device B 均只需配置一个 VLAN 接口，即可满足组网需求，从而节省 IP 资源。

在 Device A 上进行 PVLAN 和 VRRP 的配置：

- 配置 VLAN 30 为 Primary VLAN，VLAN 301～303 为其对应的 Secondary VLAN。
- 创建 VLAN 接口 30，将 VLAN 301～303 加入 VLAN 30 对应的 PVLAN L3 域，配置 VLAN 接口 30 的 IP 地址为 10.1.1.1/24。
- 配置 GigabitEthernet1/0/1 在 VLAN 301～303 中工作在 Trunk secondary 模式。
- 创建 VRRP 备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.111/24。
- 配置 Device A 在备份组 1 中的优先级为 110，高于 Device B 的优先级 100，以保证 Device A 成为 Master 负责转发。
- 配置 Device A 工作在抢占方式，以保证 Device A 故障恢复后，能再次抢占成为 Master，即只要 Device A 正常工作，就由 Device A 负责转发流量。为了避免频繁地进行状态切换，配置抢占延迟时间为 5 秒。

在 Device B 上进行 PVLAN 和 VRRP 的配置：

- 配置 VLAN 30 为 Primary VLAN，VLAN 301～303 为其对应的 Secondary VLAN。
- 创建 VLAN 接口 30，将 VLAN 301～303 加入 VLAN 30 对应的 PVLAN L3 域，配置 VLAN 接口 30 的 IP 地址为 10.1.1.2/24。
- 配置 GigabitEthernet1/0/1 在 VLAN 301～303 中工作在 Trunk secondary 模式。
- 创建 VRRP 备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.111/24。
- 配置 Device B 在备份组 1 中的优先级为 100。
- 配置 Device B 工作在抢占方式，抢占延迟时间为 5 秒。

在 Host A 上配置缺省网关为 10.1.1.111/24。

3.1.3 PVLAN 与组播应用

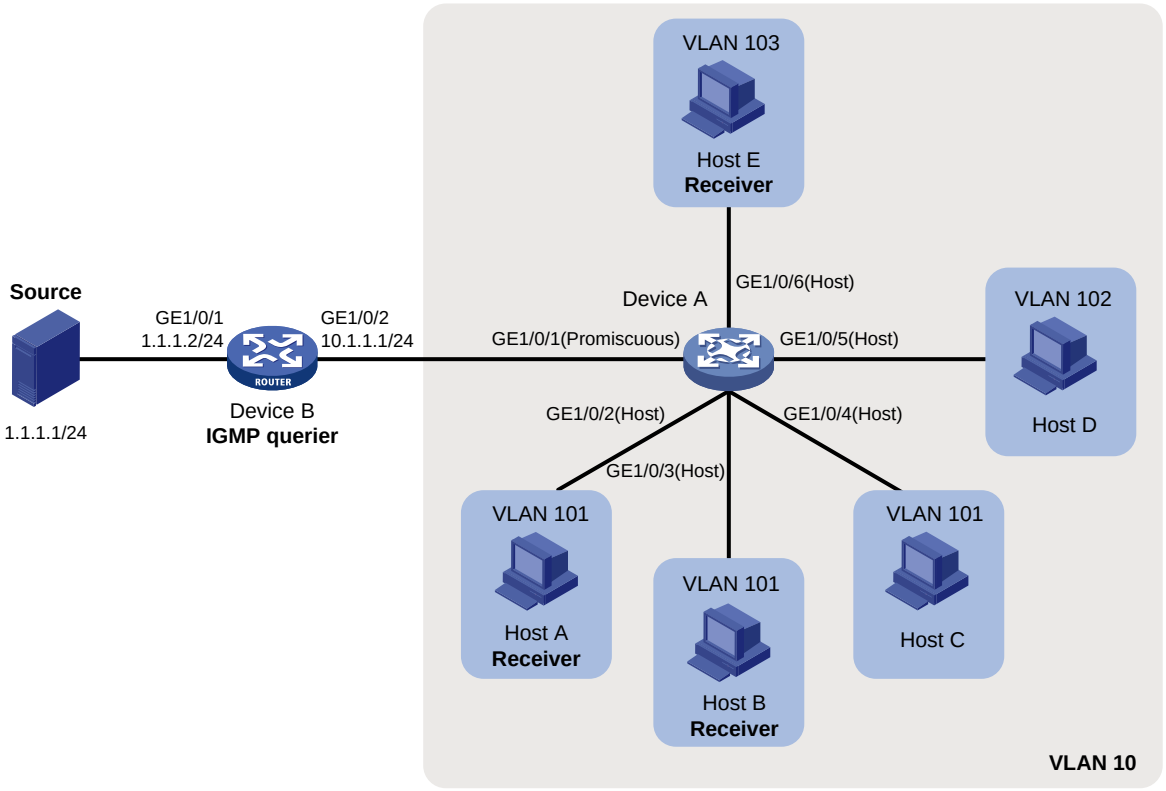
1. 二层组播

基于 PVLAN 组网要求端口均加入 Primary VLAN 的特点，二层组播可以在 Primary VLAN 上进行配置，实现二层组播支持 PVLAN 的功能。在 Primary VLAN 上进行的二层组播配置，会分发到与其建立映射的 Secondary VLAN 上，相当于一组 Private VLAN 均进行了同样的二层组播配置。PVLAN 内的组播流量（包括数据报文和协议报文）在设备内均在 Primary VLAN 内进行转发，组播表项都维护在 Primary VLAN 中。

如图 14 所示，在二层组播支持 PVLAN 组网中，进行如下配置：

- 在 Device A 上配置 Primary VLAN 10，VLAN 101、VLAN 102 和 VLAN 103 为其对应的 Secondary VLAN。
- 配置 Device A 的 GigabitEthernet1/0/1 在 Primary VLAN 10 中工作在 Promiscuous 工作模式；GigabitEthernet1/0/2、GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 加入 Secondary VLAN 101，并工作在 Host 模式；GigabitEthernet1/0/5 加入 Secondary VLAN 102，并工作在 Host 模式；GigabitEthernet1/0/6 加入 Secondary VLAN 103，并工作在 Host 模式。
- 在 Device A 上配置丢弃未知组播数据。
- Device B 通过 GigabitEthernet1/0/1 连接组播源（Source），通过 GigabitEthernet1/0/2 连接 Device A。
- Device B 上运行 IGMP（Internet Group Management Protocol，互联网组管理协议）（IGMP 版本为 IGMPv2），Device A 上运行 IGMP Snooping（IGMP Snooping 版本为 2），并由 Device B 充当 IGMP 查询器。
- Host A、Host B 和 Host E 为组播组 224.1.1.1 的固定接收者（Receiver）。

图14 二层组播支持 PVLAN 组网图

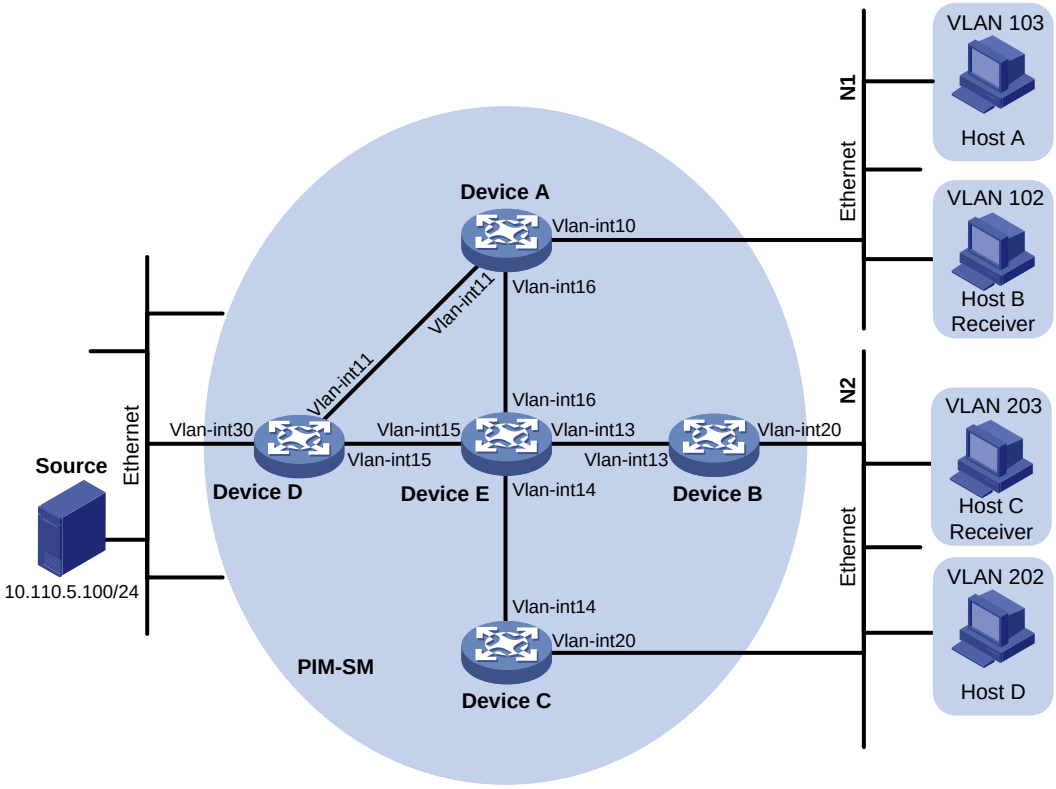


通过配置，使 Host A、Host B 和 Host E 能且只能接收发往组播组 224.1.1.1 的组播数据，并且当 Host A、Host B 和 Host E 发生意外而临时中断接收组播数据时，发往组播组 224.1.1.1 组播数据也能不间断地通过 Device A 的接口 GigabitEthernet1/0/2、GigabitEthernet1/0/3 和 GigabitEthernet1/0/6 转发出去；同时，使 Device A 将收到的未知组播数据直接丢弃，避免在其所属的 Primary VLAN 10 内广播。

2. 三层组播

三层组播与 PVLAN L3 域一起配合使用，在 Primary VLAN 的 VLAN 接口上配置三层组播协议。配置完成后，组播流量（包括数据报文和协议报文）均上送 Primary VLAN 接口，三层组播表项维护在 Primary VLAN 接口上。

图15 三层组播支持 PVLAN 组网图



设备	接口	IP地址	设备	接口	IP地址
Device A	Vlan-int10	10.110.1.1/24	Device D	Vlan-int30	10.110.5.1/24
	Vlan-int11	192.168.1.1/24		Vlan-int11	192.168.1.2/24
	Vlan-int16	192.168.9.1/24		Vlan-int15	192.168.4.2/24
Device B	Vlan-int20	10.110.2.1/24	Device E	Vlan-int14	192.168.3.2/24
	Vlan-int13	192.168.2.1/24		Vlan-int13	192.168.2.2/24
Device C	Vlan-int20	10.110.2.2/24		Vlan-int15	192.168.4.1/24
	Vlan-int14	192.168.3.1/24		Vlan-int16	192.168.9.2/24

在如图 15 所示的三层组播与 PVLAN 组网中，接收者通过组播方式接收视频点播信息，不同组织的接收者群体组成末梢网络，每个末梢网络中都存在至少一个接收者，整个 PIM 域采用 SM 非管理域方式。对组网进行如下配置：

- Host B 和 Host C 为两个末梢网络中的组播信息接收者。
- Device D 通过 VLAN 接口 30 与组播源（Source）所在网络连接。
- Device A 通过 VLAN 接口 10 连接末梢网络 N1，通过 VLAN 接口 11 和 VLAN 接口 16 分别连接 Device D 和 Device E。在 Device A 上配置 VLAN 10 为 Primary VLAN，VLAN 102 和 VLAN 103 为其 Secondary VLAN，并且 Secondary VLAN 102 与 Secondary VLAN 103 均加入 Primary VLAN 10 对应的 PVLAN L3 域。
- Device B 通过 VLAN 接口 20 连接末梢网络 N2，通过 VLAN 接口 13 连接 Device E。在 Device B 上配置 VLAN 20 为 Primary VLAN，VLAN 202 和 VLAN 203 为其 Secondary VLAN，并且 Secondary VLAN 202 与 Secondary VLAN 203 均加入 Primary VLAN 20 对应的 PVLAN L3 域。
- Device C 通过 VLAN 接口 20 连接末梢网络 N2，通过 VLAN 接口 14 连接 Device E。在 Device C 上配置 VLAN 20 为 Primary VLAN，VLAN 202 和 VLAN 203 为其 Secondary VLAN，并且

Secondary VLAN 202 与 Secondary VLAN 203 均加入 Primary VLAN 20 对应的 PVLAN L3 域。

- 将 Device E 的 VLAN 接口 16 配置为 C-BSR（Candidate Bootstrap Router，候选自举路由器）和 C-RP（Candidate Rendezvous Point，候选汇集点），其中 C-RP 所服务的组播组范围为 225.1.1.0/24。
- 在所有设备上将 Device D 的 VLAN 接口 11 配置为静态 RP（Rendezvous Point，汇集点），以对动态 RP 进行备份。Device A 与末梢网络 N1 之间运行 IGMPv2；Device B 和 Device C 与末梢网络 N2 之间也运行 IGMPv2。