

# 目 录

1 VLAN映射.....	1-1
1.1 VLAN映射简介.....	1-1
1.1.1 VLAN映射的应用.....	1-1
1.1.2 VLAN映射实现方式.....	1-3
1.2 VLAN映射配置任务简介.....	1-6
1.3 配置VLAN映射.....	1-7
1.3.1 配置 1:1 VLAN映射.....	1-7
1.3.2 配置N:1 VLAN映射（通过DHCP获取IP地址环境）.....	1-7
1.3.3 配置N:1 VLAN映射（手动配置IP地址环境）.....	1-10
1.3.4 配置 1:2 VLAN映射.....	1-11
1.3.5 配置 0:2 VLAN映射.....	1-12
1.3.6 配置 2:2 VLAN映射.....	1-13
1.4 VLAN映射显示和维护.....	1-14
1.5 VLAN映射典型配置举例.....	1-14
1.5.1 1:1 和N:1 VLAN映射配置举例.....	1-14
1.5.2 1:2 和 2:2 VLAN映射配置举例.....	1-18

# 1 VLAN映射

## 1.1 VLAN映射简介

VLAN 映射(VLAN Mapping)也叫做 VLAN 转换(VLAN Translation),它可以修改报文携带的 VLAN Tag 或为报文添加 VLAN Tag,实现不同 VLAN ID 之间的相互转换。目前设备提供下面几种映射关系:

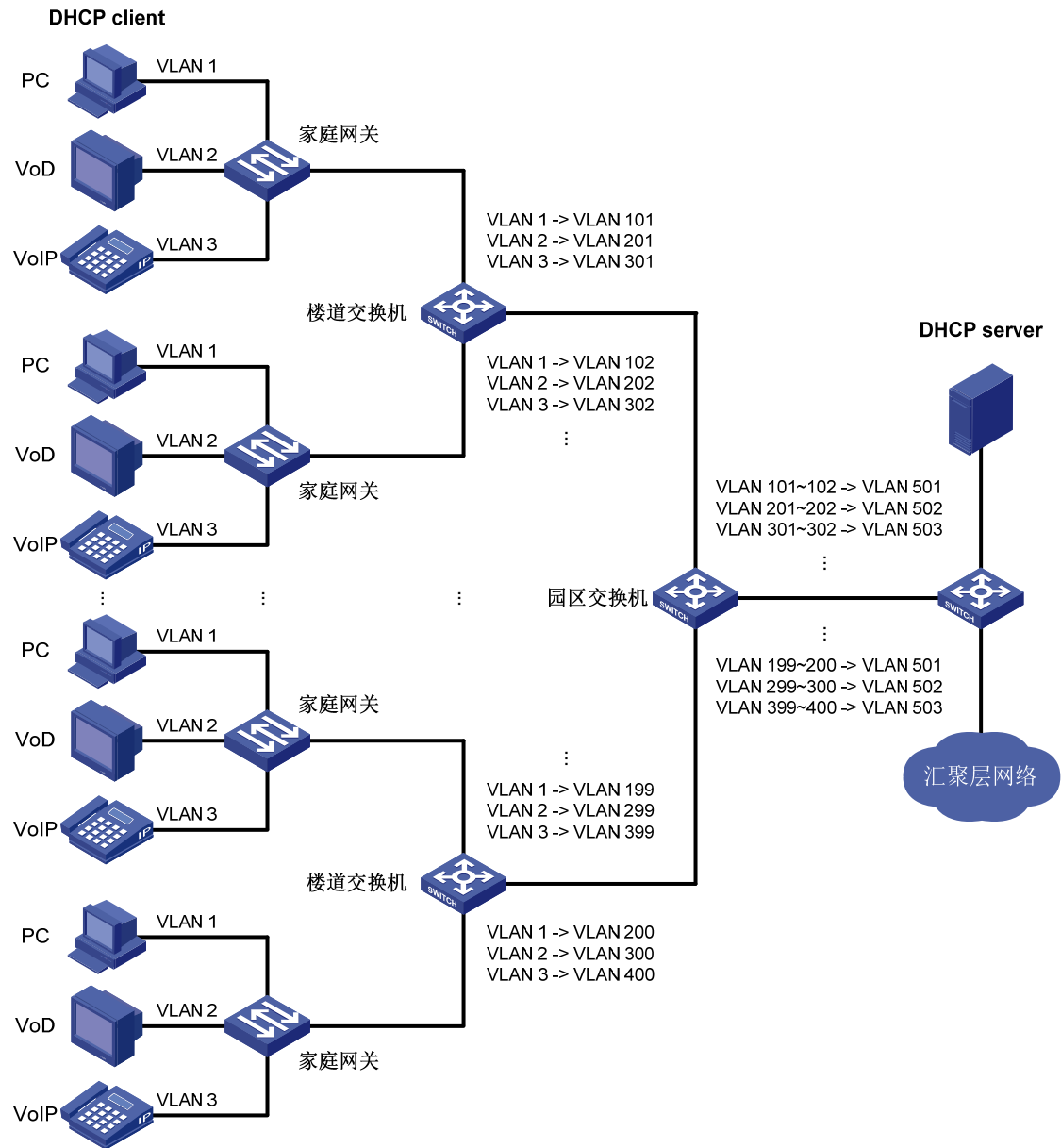
- 1:1 VLAN 映射:将来自某一特定 VLAN 的报文所携带的 VLAN Tag 替换为新的 VLAN Tag。
- N:1 VLAN 映射:将来自多个 VLAN 的报文所携带的不同 VLAN Tag 替换为相同的 VLAN Tag。
- 1:2 VLAN 映射:为携带有一层 VLAN Tag 的报文添加外层 VLAN Tag,使报文携带两层 VLAN Tag。
- 0:2 VLAN 映射:为没有携带 VLAN Tag 的报文添加两层 VLAN Tag。
- 2:2 VLAN 映射:将携带有两层 VLAN Tag 的报文的内、外层 VLAN Tag 都替换为新的 VLAN Tag。

### 1.1.1 VLAN映射的应用

#### 1.1.1.1 和N:1 VLAN映射的应用

1:1 和N:1 VLAN映射的应用环境如 [图 1-1](#)所示,小区实现宽带上网业务。

图1-1 1:1 和 N:1 VLAN 映射应用示意图



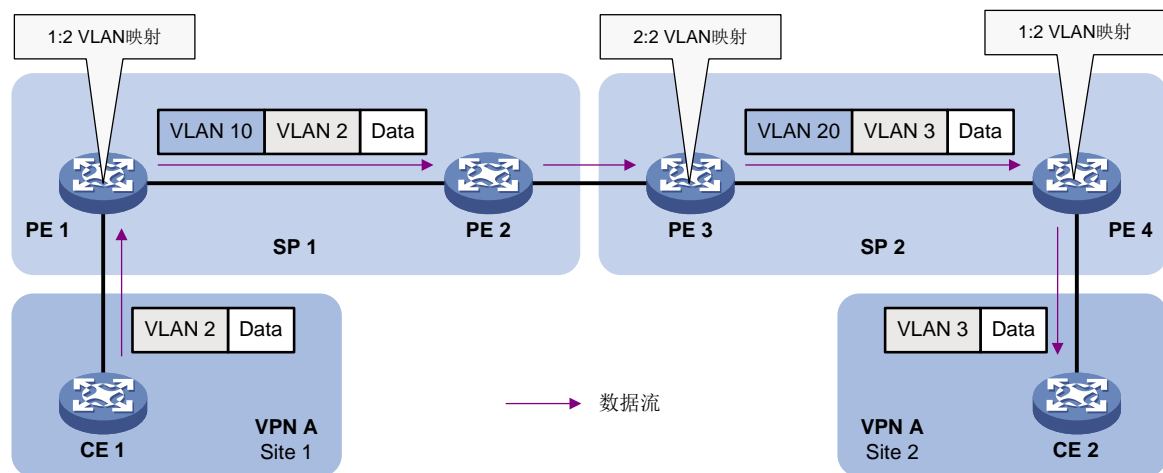
在图 1-1 中，进行了如下网络规划：

- 在家庭网关上，分别将电脑上网（PC）、视频点播（VoD）和语音电话（VoIP）业务依次划分到不同 VLAN。
- 在楼道交换机上，为了隔离不同家庭的同类业务，需要将每个家庭的每种业务都划分到不同的 VLAN，即进行 1:1 VLAN 映射，这就要用到大量的 VLAN。
- 在园区交换机上，因为汇聚层网络接入设备可提供的 VLAN 数量有限，为了节省 VLAN 资源，需要进行 VLAN 的汇聚，将所有家庭的同类业务都划分到相同的 VLAN，即进行 N:1 VLAN 映射。

## 2. 1:2 和 2:2 VLAN映射的应用

1:2 和 2:2 VLAN映射的应用环境如 图 1-2 所示，VPN A中处于不同地理位置（Site 1 和Site 2）的用户跨越了两个SP（Service Provider，服务提供商）——SP 1 和SP 2 的网络进行互通。

图1-2 1:2 和 2:2 VLAN 映射应用示意图



在 图 1-2 中，Site 1 和Site 2 中的用户所在的VLAN分别为VLAN 2 和VLAN 3，SP 1 和SP 2 分配给VPN A的VLAN分别为VLAN 10 和VLAN 20。当Site 1 的报文进入SP 1 的网络后，PE 1 为该报文添加了VLAN 10 的VLAN Tag，这个过程就是 1:2 VLAN映射。这样，VPN用户就可以自由规划自己网络中的VLAN ID，而不用担心与SP的VLAN ID相冲突，同时也因为此时报文携带两层VLAN Tag，网络可用的VLAN为  $4094 \times 4094$  个，缓解了原先SP网络中可用VLAN只有 4094 个带来的VLAN资源紧缺的问题。

当上述报文继续由 SP 1 的网络进入 SP 2 的网络后，由于 SP 2 分配给 VPN A 的 VLAN 与 SP 1 不同，另外为了实现 Site 1 与 Site 2 中的用户互通，需要同时修改该报文的内、外层 VLAN Tag，也就是进行 2:2 VLAN 映射。具体过程为，在 PE 3 上需将该报文的内层 VLAN Tag 替换为 VLAN 20 的 VLAN Tag，同时将其内层 VLAN Tag 替换为 VLAN 3 的 VLAN Tag。

## 3. 0:2 VLAN映射的应用

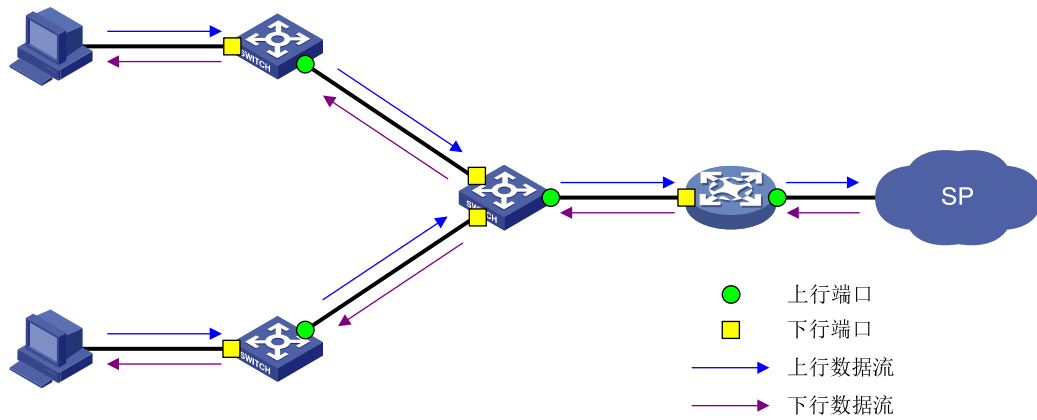
与 1:2 VLAN 映射类似，但适用于原始报文不带 VLAN Tag，组网需求需要为报文添加两层 VLAN Tag 的情况。

### 1.1.2 VLAN映射实现方式

如 图 1-3 所示，VLAN映射有如下相关概念：

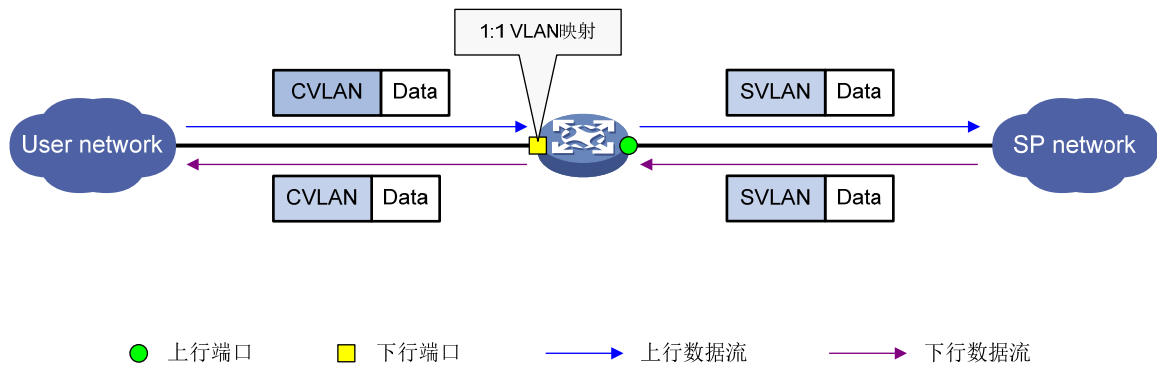
- 上行数据流：从用户网络发往汇聚层网络或 SP 网络的数据流。
- 下行数据流：从汇聚层网络或 SP 网络发往用户网络的数据流。
- 上行端口：发送上行数据流和接收下行数据流的端口。
- 下行端口：发送下行数据流和接收上行数据流的端口。

图1-3 VLAN 映射相关概念示意图



### 1. 1:1 VLAN映射实现方式

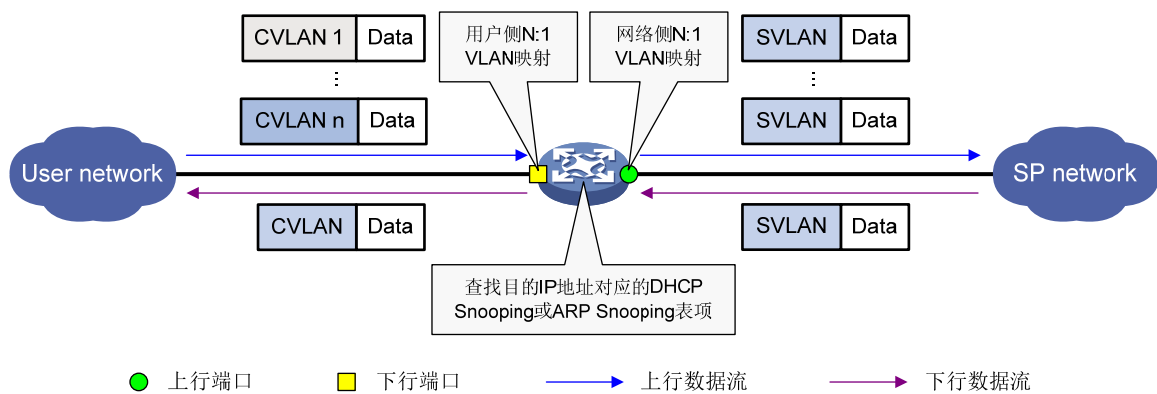
图1-4 1:1 VLAN 映射实现方式示意图



如 图 1-4 所示，通过在下行端口配置 1:1 VLAN 映射，设备将上行数据流的 CVLAN 替换为 SVLAN，将下行数据流的 SVLAN 替换为 CVLAN。

### 2. N:1 VLAN映射实现方式

图1-5 N:1 VLAN 映射实现方式示意图

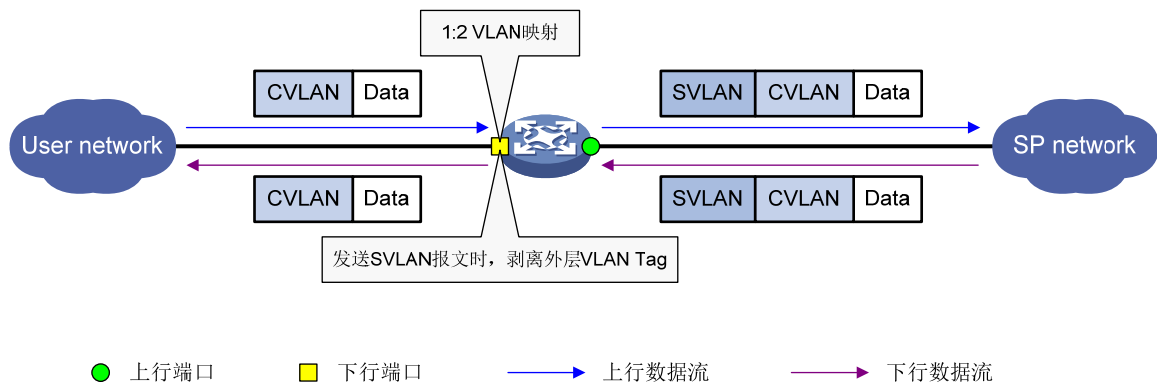


如 图 1-5 所示，N:1 VLAN 映射的实现方式如下：

- 对于上行数据流，通过在下行端口上配置用户侧 N:1 VLAN 映射，设备将来自多个 CVLAN 的报文所携带的不同 VLAN Tag 都替换为同一个 SVLAN 的 VLAN Tag。
- 对于下行数据流，通过在上行端口上配置网络侧 N:1 VLAN 映射，设备查找 DHCP Snooping 或 ARP Snooping 表项，将报文中 SVLAN 的 VLAN Tag 替换为 CVLAN 的 VLAN Tag。有关 DHCP Snooping 的详细介绍，请参见“三层技术-IP 业务配置指导”中的“DHCP Snooping”。有关 ARP Snooping 的详细介绍，请参见“三层技术-IP 业务配置指导”中的“ARP Snooping”。

### 3. 1:2 VLAN映射实现方式

图1-6 1:2 VLAN 映射实现方式示意图



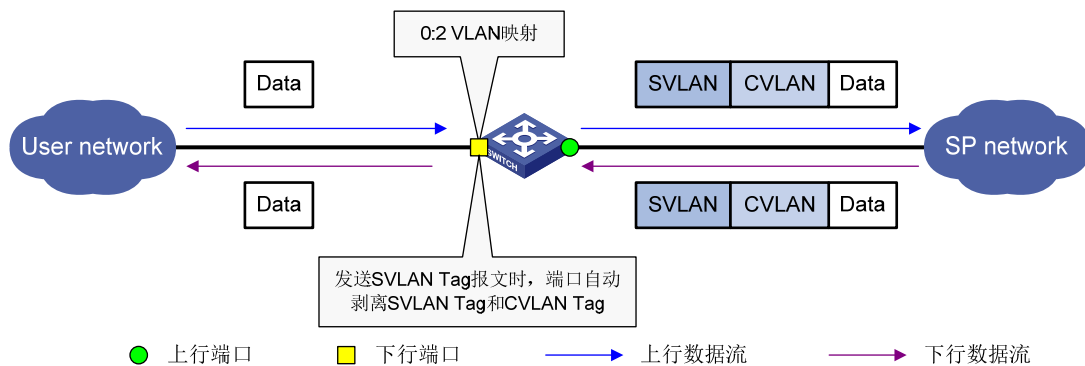
如 [图 1-6](#) 所示，通过在下行端口上配置 1:2 VLAN 映射，设备为上行数据流的 CVLAN 报文再添加一层 SVLAN 的 VLAN Tag。

配置 1:2 VLAN 映射时，为保证下行数据流可以顺利到达用户网络，在发送 SVLAN 报文时，需要剥离其外层 VLAN Tag，只保留 CVLAN Tag。可选择如下两种方式的一种来实现剥离外层 VLAN Tag：

- 配置下行端口为 Hybrid 端口，并配置当该端口发送 SVLAN 报文时不带 VLAN Tag。
- 配置下行端口成 Trunk 端口，并将 SVLAN 设为该端口的 PVID。

### 4. 0:2 VLAN映射实现方式

图1-7 0:2 VLAN 映射实现方式示意图

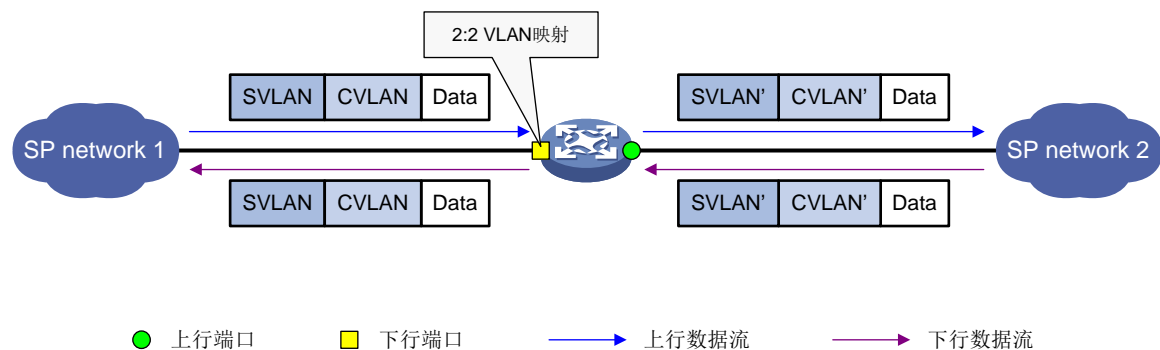


如 [图 1-7](#) 所示，0:2 VLAN 映射的实现方式如下：

- 对于上行数据流，通过在下行端口上配置 0:2 VLAN 映射，设备为端口收到的 Untagged 报文添加两层 VLAN Tag。需要注意的是，为确保 0:2 VLAN 映射生效，下行端口的 PVID 必须配置为 SVLAN。
- 对于下行数据流，设备将在下行端口自动剥离 SVLAN Tag 和 CVLAN Tag。其中，为实现剥离 SVLAN Tag，需要从如下三种方式中选择一种：
  - 配置下行端口为 Access 端口，将该端口加入 SVLAN。
  - 配置下行端口为 Trunk 端口，允许 SVLAN 通过并将 SVLAN 设为该端口的 PVID。
  - 配置下行端口为 Hybrid 端口，允许 SVLAN 通过并将 SVLAN 设为该端口的 PVID，同时配置当该端口发送 SVLAN 报文时不携带 VLAN Tag。

### 5. 2:2 VLAN映射实现方式

图1-8 2:2 VLAN 映射实现方式示意图



如 图 1-8 所示，通过在下行端口配置 2:2 VLAN 映射，设备将上行数据流的 SVLAN、CVLAN 转换为 SVLAN'、CVLAN'，将下行数据流的 SVLAN'、CVLAN' 转换为 SVLAN、CVLAN。

## 1.2 VLAN映射配置任务简介

用户需要根据网络规划，在不同的设备上进行不同的 VLAN 映射配置。

配置 VLAN 映射时，需要注意：

- 若用户同时通过配置 VLAN 映射和 QinQ 来添加报文的 VLAN Tag，且配置冲突时，VLAN 映射的配置生效。有关 QinQ 的详细介绍，请参见“二层技术-以太网交换”中的“QinQ”。
- 若用户同时通过配置 VLAN 映射和 QoS 策略来修改或添加报文的 VLAN Tag，且配置冲突时，QoS 策略的配置生效。有关 QoS 策略的详细介绍，请参见“ACL 和 QoS 配置指导”中的“QoS 配置方式”。

表1-1 VLAN 映射配置任务简介

配置任务	说明	详细配置
配置1:1 VLAN映射	在图1-1所示的组网中，需要在楼道交换机上进行此配置	<a href="#">1.3.1</a>
配置N:1 VLAN映射（通过DHCP获取IP地址环境）	在图1-1所示的组网中，需要在园区交换机上进行此配置	<a href="#">1.3.2</a>
配置N:1 VLAN映射（手动配置IP地址环境）	在图1-1所示的组网中，需要在园区交换机上进行此配置	<a href="#">1.3.3</a>

配置任务	说明	详细配置
配置1:2 VLAN映射	在图1-2所示的组网中，需要在用户进入SP网络的边缘设备PE 1和PE 4上进行此配置	<a href="#">1.3.4</a>
配置0:2 VLAN映射	-	<a href="#">1.3.5</a>
配置2:2 VLAN映射	在图1-2所示的组网中，需要在SP 2网络的边缘设备PE 3上进行此配置	<a href="#">1.3.6</a>

## 1.3 配置VLAN映射

### 1.3.1 配置 1:1 VLAN映射

在图1-1所示的组网中，需要在楼道交换机上配置 1:1 VLAN映射，以便将不同用户的不同业务用不同的VLAN进行隔离。

在配置 1:1 VLAN 映射前，需要先创建好原始 VLAN 和转换后 VLAN。

1:1 VLAN 映射需要在设备下行端口上进行配置。

表1-2 配置 1:1 VLAN 映射

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入相应视图	<ul style="list-style-type: none"> <li>进入二层以太网接口视图： <b>interface interface-type interface-number</b></li> <li>进入二层聚合接口视图： <b>interface bridge-aggregation interface-number</b></li> </ul>	-
配置端口链路类型	<ul style="list-style-type: none"> <li>配置端口的链路类型为 Trunk 类型： <b>port link-type trunk</b></li> <li>配置端口的链路类型为 Hybrid 类型： <b>port link-type hybrid</b></li> </ul>	二者选其一 缺省情况下，所有端口的链路类型均为Access类型
配置允许原始VLAN及转换后VLAN通过当前端口	<ul style="list-style-type: none"> <li><b>port trunk permit vlan vlan-id-list</b></li> <li><b>port hybrid vlan vlan-id-list tagged</b></li> </ul>	二者选其一
配置1:1 VLAN映射	<b>vlan mapping vlan-id translated-vlan vlan-id</b>	缺省情况下，接口上未配置VLAN映射

### 1.3.2 配置N:1 VLAN映射（通过DHCP获取IP地址环境）

在图1-1所示的组网中，需要在园区交换机上配置N:1 VLAN映射，以便将不同用户的相同业务用同一个VLAN进行发送，从而节省VLAN资源。

#### 1. 配置任务简介

在配置 N:1 VLAN 映射前，需要先创建好原始 VLAN 和转换后 VLAN。



需要注意的是，该功能不能与 uRPF（Unicast Reverse Path Forwarding，单播反向路径转发）功能同时使用，否则会造成网络侧发往用户侧的流量不能正常转发。有关 uRPF 的详细介绍，请参见“安全配置指导”中的“uRPF”。

N:1 VLAN 映射配置中，DHCP Snooping 相关命令的详细介绍，请参见“三层技术-IP 业务命令参考”中的“DHCP Snooping”；ARP Detection 相关命令的详细介绍，请参见“安全命令参考”中的“ARP 攻击防御”。

如果用户想改变 N:1 VLAN 映射关系，必须先用 **reset dhcp snooping binding** 命令清除 DHCP Snooping 表项，然后再修改 N:1 VLAN 映射关系。

表1-3 N:1 VLAN 映射配置任务简介

配置任务	说明	详细配置
使能DHCP Snooping功能	必选	<a href="#">1.3.2 2.</a>
使能ARP Detection功能	必选	<a href="#">1.3.2 3.</a>
配置下行端口	必选	<a href="#">1.3.2 4.</a>
配置上行端口	必选	<a href="#">1.3.2 5.</a>

## 2. 使能DHCP Snooping功能

表1-4 使能 DHCP Snooping 功能

操作	命令	说明
进入系统视图	<b>system-view</b>	-
使能DHCP Snooping功能	<b>dhcp snooping enable</b>	缺省情况下，DHCP Snooping功能处于关闭状态

## 3. 使能ARP Detection功能

请在所有需要进行映射的 VLAN(包括原始 VLAN 和转换后 VLAN)上都使能 ARP Detection 功能。

表1-5 使能 ARP Detection 功能

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入VLAN视图	<b>vlan <i>vlan-id</i></b>	-
使能ARP Detection功能	<b>arp detection enable</b>	缺省情况下，ARP Detection功能处于关闭状态

## 4. 配置下行端口

表1-6 配置下行端口

操作	命令	说明
进入系统视图	<b>system-view</b>	-

操作	命令	说明
进入相应视图	<ul style="list-style-type: none"> <li>进入二层以太网接口视图： <b>interface interface-type interface-number</b></li> <li>进入二层聚合接口视图： <b>interface bridge-aggregation interface-number</b></li> </ul>	-
配置端口链路类型	<ul style="list-style-type: none"> <li>配置端口的链路类型为 Trunk 类型： <b>port link-type trunk</b></li> <li>配置端口的链路类型为 Hybrid 类型： <b>port link-type hybrid</b></li> </ul>	二者选其一 缺省情况下，所有端口的链路类型均为Access类型
配置允许原始VLAN及转换后VLAN通过当前端口	<ul style="list-style-type: none"> <li><b>port trunk permit vlan vlan-id-list</b></li> <li><b>port hybrid vlan vlan-id-list tagged</b></li> </ul>	二者选其一
配置用户侧N:1 VLAN映射	<b>vlan mapping uni { range vlan-range-list   single vlan-id-list } translated-vlan vlan-id</b>	缺省情况下，接口上未配置VLAN映射
开启端口的DHCP Snooping表项记录功能	<b>dhcp snooping binding record</b>	缺省情况下，接口的DHCP Snooping表项记录功能处于关闭状态

## 5. 配置上行端口

表1-7 配置上行端口

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入相应视图	<ul style="list-style-type: none"> <li>进入二层以太网接口视图： <b>interface interface-type interface-number</b></li> <li>进入二层聚合接口视图： <b>interface bridge-aggregation interface-number</b></li> </ul>	-
配置端口链路类型	<ul style="list-style-type: none"> <li>配置端口的链路类型为 Trunk 类型： <b>port link-type trunk</b></li> <li>配置端口的链路类型为 Hybrid 类型： <b>port link-type hybrid</b></li> </ul>	二者选其一 缺省情况下，所有端口的链路类型均为Access类型
配置允许转换后VLAN通过当前端口	<ul style="list-style-type: none"> <li><b>port trunk permit vlan vlan-id-list</b></li> <li><b>port hybrid vlan vlan-id-list tagged</b></li> </ul>	二者选其一
配置端口为DHCP信任端口	<b>dhcp snooping trust</b>	缺省情况下，在使能DHCP Snooping功能后，设备上所有支持DHCP Snooping功能的端口均为不信任端口
配置端口为ARP信任端口	<b>arp detection trust</b>	缺省情况下，接口为ARP非信任接口
配置网络侧N:1 VLAN映射	<b>vlan mapping nni</b>	缺省情况下，接口上未配置VLAN映射

### 1.3.3 配置N:1 VLAN映射（手动配置IP地址环境）

在手动配置 IP 地址的环境中，配置 N:1 VLAN 映射功能需要配合使用 ARP Snooping 功能。设备通过查找 ARP Snooping 表项，可以将下行数据流报文中 SVLAN 的 VLAN Tag 替换为 CVLAN 的 VLAN Tag。

#### 1. 配置任务简介

在配置 N:1 VLAN 映射前，需要先创建好原始 VLAN 和转换后 VLAN。

配置 N:1 VLAN 映射时，需要注意的是：

- 该功能不能与 uRPF 功能同时使用，否则会造成网络侧发往用户侧的流量不能正常转发。有关 uRPF 的详细介绍，请参见“安全配置指导”中的“uRPF”。
- 不同的 CVLAN 内不能配置有相同的 IP 地址。
- 如果同一 VLAN 内同一 IP 地址对应的 MAC 地址发生变化，会造成冲突，使 ARP Snooping 表项失效。此时可以使用 **reset arp snooping** 命令清除指定 IP 地址的 ARP Snooping 表项或等待表项老化。
- 如果用户想改变 N:1 VLAN 映射关系，必须先用 **reset arp snooping** 命令清除所涉及 VLAN 的 ARP Snooping 表项，然后再修改 N:1 VLAN 映射关系。
- ARP Snooping 相关命令的详细介绍，请参见“三层技术-IP 业务命令参考/ARP”中的“ARP Snooping”。

表1-8 N:1 VLAN 映射配置任务简介

配置任务	说明	详细配置
使能ARP Snooping功能	必选	<a href="#">1.3.3 2.</a>
配置下行端口	必选	<a href="#">1.3.3 3.</a>
配置上行端口	必选	<a href="#">1.3.3 4.</a>

#### 2. 使能ARP Snooping功能

请在所有需要进行映射的 VLAN(包括原始 VLAN 和转换后 VLAN)上都使能 ARP Snooping 功能。

表1-9 使能 ARP Snooping 功能

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入VLAN视图	<b>vlan <i>vlan-id</i></b>	-
使能ARP Snooping功能	<b>arp snooping enable</b>	缺省情况下，ARP Snooping功能处于关闭状态

#### 3. 配置下行端口

表1-10 配置下行端口

操作	命令	说明
进入系统视图	<b>system-view</b>	-

操作	命令	说明
进入相应视图	<ul style="list-style-type: none"> <li>进入二层以太网接口视图： <b>interface interface-type interface-number</b></li> <li>进入二层聚合接口视图： <b>interface bridge-aggregation interface-number</b></li> </ul>	-
配置端口链路类型	<ul style="list-style-type: none"> <li>配置端口的链路类型为 Trunk 类型： <b>port link-type trunk</b></li> <li>配置端口的链路类型为 Hybrid 类型： <b>port link-type hybrid</b></li> </ul>	二者必选其一 缺省情况下，所有端口的链路类型均为Access类型
配置允许原始VLAN及转换后VLAN通过当前端口	<ul style="list-style-type: none"> <li><b>port trunk permit vlan vlan-id-list</b></li> <li><b>port hybrid vlan vlan-id-list tagged</b></li> </ul>	二者必选其一
配置用户侧N:1 VLAN映射	<b>vlan mapping uni { range vlan-range-list   single vlan-id-list } translated-vlan vlan-id</b>	缺省情况下，接口上未配置VLAN映射

#### 4. 配置上行端口

表1-11 配置上行端口

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入相应视图	<ul style="list-style-type: none"> <li>进入二层以太网接口视图： <b>interface interface-type interface-number</b></li> <li>进入二层聚合接口视图： <b>interface bridge-aggregation interface-number</b></li> </ul>	-
配置端口链路类型	<ul style="list-style-type: none"> <li>配置端口的链路类型为 Trunk 类型： <b>port link-type trunk</b></li> <li>配置端口的链路类型为 Hybrid 类型： <b>port link-type hybrid</b></li> </ul>	二者必选其一 缺省情况下，所有端口的链路类型均为Access类型
配置允许转换后VLAN通过当前端口	<ul style="list-style-type: none"> <li><b>port trunk permit vlan vlan-id-list</b></li> <li><b>port hybrid vlan vlan-id-list tagged</b></li> </ul>	二者必选其一
配置网络侧N:1 VLAN映射	<b>vlan mapping nni</b>	缺省情况下，接口上未配置VLAN映射

#### 1.3.4 配置 1:2 VLAN映射

在图 1-2 所示的组网中，需要在用户进入SP网络的边缘设备PE 1 和PE 4 上配置 1:2 VLAN映射，以便为报文添加SP分配给用户的外层VLAN Tag，使得不同用户的报文在SP网络中传输时被完全隔离。

在配置 1:2 VLAN 映射前，需要先创建好原始 VLAN 和转换后 VLAN。

需要注意的是，1:2 VLAN 映射为报文加上外层 VLAN Tag 后，内层 VLAN Tag 将被当作报文的数据部分进行传输，报文长度将增加 4 个字节。因此建议用户适当增加映射后报文传输路径上各接口的 MTU（Maximum Transmission Unit，最大传输单元）值（至少为 1504 字节）。

1:2 VLAN 映射需要在设备下行端口上进行配置。

表1-12 配置 1:2 VLAN 映射

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入相应视图	<ul style="list-style-type: none"> <li>进入二层以太网接口视图： <b>interface interface-type interface-number</b></li> <li>进入二层聚合接口视图： <b>interface bridge-aggregation interface-number</b></li> </ul>	-
配置端口的链路类型	<ul style="list-style-type: none"> <li>配置端口的链路类型为 Trunk 类型： <b>port link-type trunk</b></li> <li>配置端口的链路类型为 Hybrid 类型： <b>port link-type hybrid</b></li> </ul>	二者选其一 缺省情况下，所有端口的链路类型均为 Access 类型
配置允许原始 VLAN 通过当前端口	<ul style="list-style-type: none"> <li><b>port trunk permit vlan vlan-id-list</b></li> <li><b>port hybrid vlan vlan-id-list { tagged   untagged }</b></li> </ul>	二者选其一
配置允许转换后外层 VLAN 不带 Tag 通过当前端口	<ul style="list-style-type: none"> <li>配置 Trunk 端口的 PVID 为添加的外层 VLAN 并允许该 VLAN 通过： <ul style="list-style-type: none"> <li><b>port trunk pvid vlan vlan-id</b></li> <li><b>port trunk permit vlan { vlan-id-list   all }</b></li> </ul> </li> <li>配置允许添加的外层 VLAN 以 Untagged 方式通过 Hybrid 端口： <b>port hybrid vlan vlan-id-list untagged</b></li> </ul>	二者选其一
配置 1:2 VLAN 映射	<b>vlan mapping nest { range vlan-range-list   single vlan-id-list } nested-vlan vlan-id</b>	缺省情况下，接口上未配置 VLAN 映射 一个原始 VLAN 只能映射一个转换后外层 VLAN。若要为不同原始 VLAN 的报文添加不同的外层 VLAN Tag，需将端口的链路类型配置为 Hybrid 类型并多次执行本命令

### 1.3.5 配置 0:2 VLAN 映射

配置 0:2 VLAN 映射时，在携带两层 VLAN Tag 的报文的传输路径上建议用户适当增加各接口的 MTU 值（至少为 1504 字节）。另外，需确保上行端口允许 SVLAN 以 Tagged 方式通过。

0:2 VLAN 映射需要在设备下行端口上进行配置。

表1-13 配置 0:2 VLAN 映射

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入相应视图	<ul style="list-style-type: none"> <li>进入二层以太网接口视图： <b>interface interface-type interface-number</b></li> <li>进入二层聚合接口视图： <b>interface bridge-aggregation interface-number</b></li> </ul>	-
配置端口的链路类型	<ul style="list-style-type: none"> <li>配置端口的链路类型为 Access 类型： <b>port link-type access</b></li> <li>配置端口的链路类型为 Trunk 类型： <b>port link-type trunk</b></li> <li>配置端口的链路类型为 Hybrid 类型： <b>port link-type hybrid</b></li> </ul>	三者选其一 缺省情况下，所有端口的链路类型均为Access类型
配置端口允许SVLAN以Untagged方式通过	<ul style="list-style-type: none"> <li>将 Access 端口加入到 SVLAN： <b>port access vlan vlan-id</b></li> <li>配置 Trunk 端口允许 SVLAN 通过，并配置 Trunk 端口的 PVID 为 SVLAN： <b>port trunk permit vlan vlan-id-list</b> <b>port trunk pvid vlan vlan-id</b></li> <li>配置 Hybrid 端口允许 SVLAN 以 Untagged 方式通过，并配置 Hybrid 端口的 PVID 为 SVLAN： <b>port hybrid vlan vlan-id-list untagged</b> <b>port hybrid pvid vlan vlan-id</b></li> </ul>	三者选其一
配置0:2 VLAN映射	<b>vlan mapping untagged nested-outer-vlan outer-vlan-id nested-inner-vlan inner-vlan-id</b>	缺省情况下，接口上未配置VLAN映射

### 1.3.6 配置 2:2 VLAN映射

在图 1-2 所示的组网中，需要在 SP 2 网络的边缘设备 PE 3 上配置 2:2 VLAN 映射，将报文外层 VLAN Tag 替换为新 SP 网络分配给同一 VPN 用户的 VLAN Tag，同时替换内层 VLAN Tag，使得该 VPN 内原本不同 VLAN 的用户可以互通。

在配置 2:2 VLAN 映射前，需要先创建好原始 VLAN 和转换后 VLAN。

2:2 VLAN 映射需要在设备下行端口上进行配置。

表1-14 配置 2:2 VLAN 映射

操作	命令	说明
进入系统视图	<b>system-view</b>	-
进入相应视图	<ul style="list-style-type: none"> <li>进入二层以太网接口视图： <b>interface interface-type interface-number</b></li> <li>进入二层聚合接口视图： <b>interface bridge-aggregation interface-number</b></li> </ul>	-

操作	命令	说明
配置端口链路类型	<ul style="list-style-type: none"> <li>配置端口的链路类型为 Trunk 类型： <b>port link-type trunk</b></li> <li>配置端口的链路类型为 Hybrid 类型： <b>port link-type hybrid</b></li> </ul>	二者选其一 缺省情况下，所有端口的链路类型均为Access类型
配置允许原始外层VLAN及转换后外层VLAN通过当前端口	<ul style="list-style-type: none"> <li><b>port trunk permit vlan <i>vlan-id-list</i></b></li> <li><b>port hybrid vlan <i>vlan-id-list</i> tagged</b></li> </ul>	二者选其一
配置2:2 VLAN映射	<b>vlan mapping tunnel <i>outer-vlan-id inner-vlan-id translated-vlan outer-vlan-id inner-vlan-id</i></b>	缺省情况下，接口上未配置VLAN映射

## 1.4 VLAN映射显示和维护

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 VLAN 映射的运行情况，通过查看显示信息验证配置的效果。

表1-15 VLAN 映射显示和维护

操作	命令
显示VLAN映射信息	<b>display vlan mapping [ interface <i>interface-type interface-number</i> ]</b>

## 1.5 VLAN映射典型配置举例

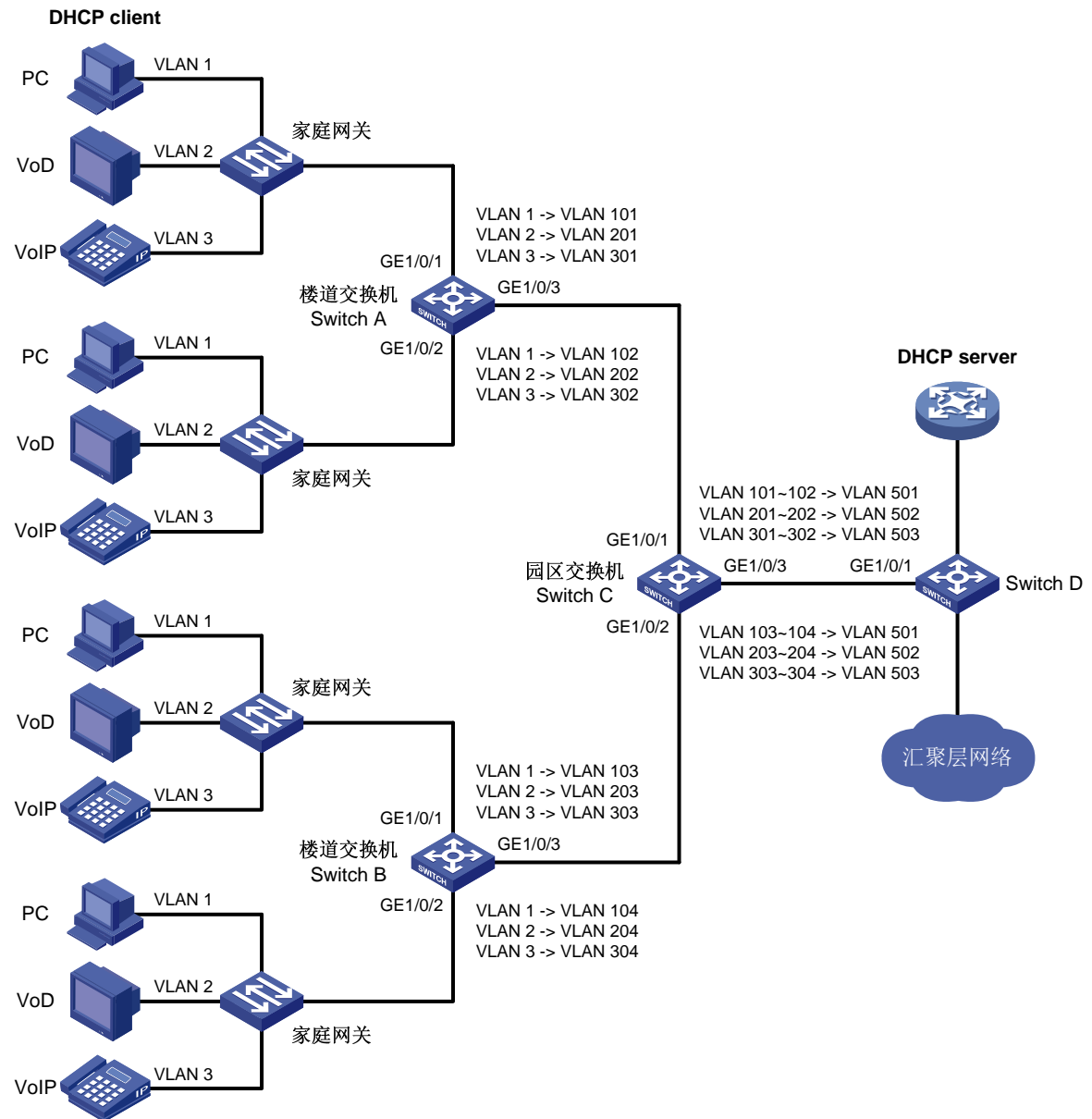
### 1.5.1 1:1 和N:1 VLAN映射配置举例

#### 1. 组网需求

- 在某小区，服务提供商为每个家庭都提供了 PC、VoD 和 VoIP 这三种数据服务，每个家庭都通过各自的家庭网关接入楼道交换机，并通过 DHCP 方式自动获取 IP 地址。
- 服务提供商希望实现以下网络规划：在家庭网关上，分别将 PC、VoD 和 VoIP 业务依次划分到 VLAN 1~3；在楼道交换机上，为了隔离不同家庭的同类业务，将每个家庭的每种业务都划分到不同的 VLAN；而在园区交换机上，为了节省 VLAN 资源，将所有家庭的同类业务都划分到相同的 VLAN，即分别将 PC、VoD 和 VoIP 业务依次划分到 VLAN 501~503。

## 2. 组网图

图1-9 1:1 和 N:1 VLAN 映射配置组网图



## 3. 配置步骤

### (1) 配置 Switch A

# 配置下行端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 为 Trunk 端口且允许原始 VLAN 及转换后 VLAN 通过，同时在端口上配置 1:1 VLAN 映射。

```
<SwitchA> system-view
[SwitchA] vlan 2 to 3
[SwitchA] vlan 101 to 102
[SwitchA] vlan 201 to 202
[SwitchA] vlan 301 to 302
[SwitchA] interface gigabitethernet 1/0/1
```



```

[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan 1 2 3 101 201 301
[SwitchA-GigabitEthernet1/0/1] vlan mapping 1 translated-vlan 101
[SwitchA-GigabitEthernet1/0/1] vlan mapping 2 translated-vlan 201
[SwitchA-GigabitEthernet1/0/1] vlan mapping 3 translated-vlan 301
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 1 2 3 102 202 302
[SwitchA-GigabitEthernet1/0/2] vlan mapping 1 translated-vlan 102
[SwitchA-GigabitEthernet1/0/2] vlan mapping 2 translated-vlan 202
[SwitchA-GigabitEthernet1/0/2] vlan mapping 3 translated-vlan 302
[SwitchA-GigabitEthernet1/0/2] quit
# 配置上行端口 GigabitEthernet1/0/3 为 Trunk 端口，且允许转换后 VLAN 通过。
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 101 201 301 102 202 302
[SwitchA-GigabitEthernet1/0/3] quit

```

## (2) 配置 Switch B

Switch B 的配置与 Switch A 相似，配置过程略。

## (3) 配置 Switch C

# 使能 DHCP Snooping 功能。

```

<SwitchC> system-view
[SwitchC] dhcp snooping enable
# 创建原始 VLAN 和转换后 VLAN，并在这些 VLAN 上分别使能 ARP Detection 功能。
[SwitchC] vlan 101
[SwitchC-vlan101] arp detection enable
[SwitchC-vlan101] vlan 201
[SwitchC-vlan201] arp detection enable
[SwitchC-vlan201] vlan 301
[SwitchC-vlan301] arp detection enable
[SwitchC-vlan301] vlan 102
[SwitchC-vlan102] arp detection enable
[SwitchC-vlan102] vlan 202
[SwitchC-vlan202] arp detection enable
[SwitchC-vlan202] vlan 302
[SwitchC-vlan302] arp detection enable
[SwitchC-vlan302] vlan 103
[SwitchC-vlan103] arp detection enable
[SwitchC-vlan103] vlan 203
[SwitchC-vlan203] arp detection enable
[SwitchC-vlan203] vlan 303
[SwitchC-vlan303] arp detection enable
[SwitchC-vlan303] vlan 104
[SwitchC-vlan104] arp detection enable
[SwitchC-vlan104] vlan 204
[SwitchC-vlan204] arp detection enable

```

```
[SwitchC-vlan204] vlan 304
[SwitchC-vlan304] arp detection enable
[SwitchC-vlan304] vlan 501
[SwitchC-vlan501] arp detection enable
[SwitchC-vlan501] vlan 502
[SwitchC-vlan502] arp detection enable
[SwitchC-vlan502] vlan 503
[SwitchC-vlan503] arp detection enable
[SwitchC-vlan503] quit
```

# 配置下行端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 为 Trunk 端口且允许原始 VLAN 及转换后 VLAN 通过，同时在端口上配置 N:1 VLAN 映射，并启用 DHCP Snooping 表项记录功能。

```
[SwitchC] interface gigabitethernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 101 102 201 202 301 302 501 to 503
[SwitchC-GigabitEthernet1/0/1] vlan mapping uni range 101 to 102 translated-vlan 501
[SwitchC-GigabitEthernet1/0/1] vlan mapping uni range 201 to 202 translated-vlan 502
[SwitchC-GigabitEthernet1/0/1] vlan mapping uni range 301 to 302 translated-vlan 503
[SwitchC-GigabitEthernet1/0/1] dhcp snooping binding record
[SwitchC-GigabitEthernet1/0/1] quit
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port link-type trunk
[SwitchC-GigabitEthernet1/0/2] port trunk permit vlan 103 104 203 204 303 304 501 to 503
[SwitchC-GigabitEthernet1/0/2] vlan mapping uni range 103 to 104 translated-vlan 501
[SwitchC-GigabitEthernet1/0/2] vlan mapping uni range 203 to 204 translated-vlan 502
[SwitchC-GigabitEthernet1/0/2] vlan mapping uni range 303 to 304 translated-vlan 503
[SwitchC-GigabitEthernet1/0/2] dhcp snooping binding record
[SwitchC-GigabitEthernet1/0/2] quit
```

# 在上行端口 GigabitEthernet1/0/3 上配置网络侧 N:1 VLAN 映射。

```
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] vlan mapping nni
```

# 配置端口 GigabitEthernet1/0/3 为 Trunk 端口且允许转换后 VLAN 通过，并配置该端口为 DHCP Snooping 信任端口和 ARP 信任端口。

```
[SwitchC-GigabitEthernet1/0/3] port link-type trunk
[SwitchC-GigabitEthernet1/0/3] port trunk permit vlan 501 to 503
[SwitchC-GigabitEthernet1/0/3] dhcp snooping trust
[SwitchC-GigabitEthernet1/0/3] arp detection trust
[SwitchC-GigabitEthernet1/0/3] quit
```

#### (4) 配置 Switch D

# 配置端口 GigabitEthernet1/0/1 为 Trunk 端口且允许转换后 VLAN 通过。

```
<SwitchD> system-view
[SwitchD] vlan 501 to 503
[SwitchD] interface gigabitethernet 1/0/1
[SwitchD-GigabitEthernet1/0/1] port link-type trunk
[SwitchD-GigabitEthernet1/0/1] port trunk permit vlan 501 to 503
[SwitchD-GigabitEthernet1/0/1] quit
```

## 4. 验证配置

### (1) 查看 Switch A 上的 VLAN 映射配置信息

```
[SwitchA] display vlan mapping
```

```
Interface GigabitEthernet1/0/1:
```

Outer VLAN	Inner VLAN	Translated Outer VLAN	Translated Inner VLAN
1	N/A	101	N/A
2	N/A	201	N/A
3	N/A	301	N/A

```
Interface GigabitEthernet1/0/2:
```

Outer VLAN	Inner VLAN	Translated Outer VLAN	Translated Inner VLAN
1	N/A	102	N/A
2	N/A	202	N/A
3	N/A	302	N/A

### (2) 查看 Switch B 上的 VLAN 映射配置信息

Switch B 上的 VLAN 映射配置信息与 Switch A 相似，显示信息略。

### (3) 查看 Switch C 上的 VLAN 映射配置信息

```
[SwitchC] display vlan mapping
```

```
Interface GigabitEthernet1/0/1:
```

Outer VLAN	Inner VLAN	Translated Outer VLAN	Translated Inner VLAN
101-102	N/A	501	N/A
201-202	N/A	502	N/A
301-302	N/A	503	N/A

```
Interface GigabitEthernet1/0/2:
```

Outer VLAN	Inner VLAN	Translated Outer VLAN	Translated Inner VLAN
103-104	N/A	501	N/A
203-204	N/A	502	N/A
303-304	N/A	503	N/A

以上信息表明，Switch A 和 Switch B 上的 1:1 VLAN 映射，以及 Switch C 上的 N:1 VLAN 映射配置成功。

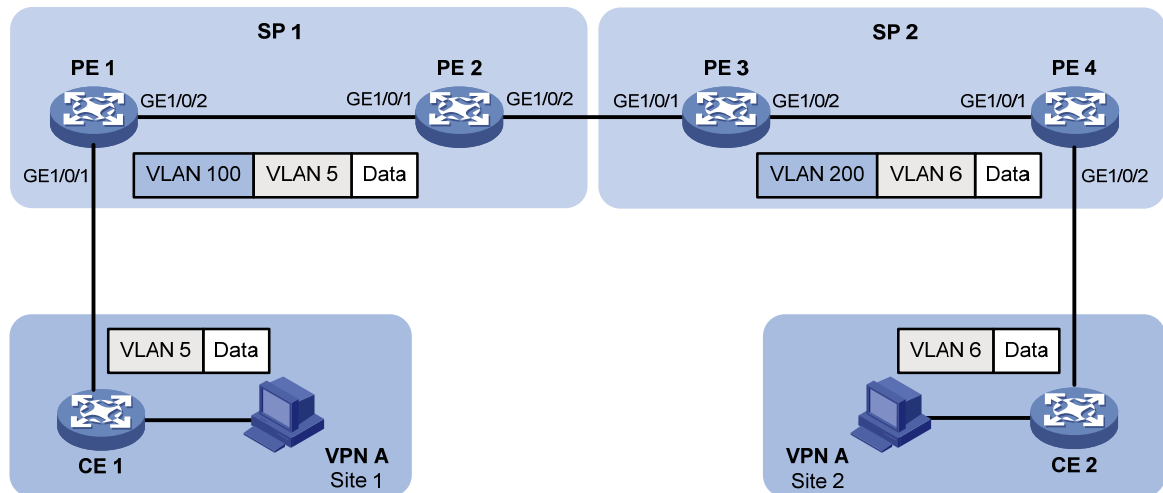
## 1.5.2 1:2 和 2:2 VLAN映射配置举例

### 1. 组网需求

- VPN A 中的 Site 1 和 Site 2 是某公司的两个分支机构，且分别利用 VLAN 5 和 VLAN 6 承载业务。由于分处不同地域，这两个分支机构采用了不同的 SP 所提供的 VPN 接入服务，SP 1 和 SP 2 分别将 VLAN 100 和 VLAN 200 分配给这两个分支机构使用。
- 该公司希望其下属的这两个分支机构可以跨越 SP 1 和 SP 2 的网络实现互通。

## 2. 组网图

图1-10 1:2 和 2:2 VLAN 映射配置组网图



## 3. 配置步骤

### (1) 配置 PE 1

# 在下行端口 GigabitEthernet1/0/1 上配置 1:2 VLAN 映射，为 VLAN 5 的报文添加 VLAN 100 的外层 VLAN Tag。

```
<PE1> system-view
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] vlan mapping nest single 5 nested-vlan 100
```

# 配置 GigabitEthernet1/0/1 为 Hybrid 端口且允许 VLAN 5 的报文携带 VLAN Tag 通过、VLAN 100 的报文不携带 VLAN Tag 通过。

```
[PE1-GigabitEthernet1/0/1] port link-type hybrid
[PE1-GigabitEthernet1/0/1] port hybrid vlan 5 tagged
[PE1-GigabitEthernet1/0/1] port hybrid vlan 100 untagged
[PE1-GigabitEthernet1/0/1] quit
```

# 配置上行端口 GigabitEthernet1/0/2 为 Trunk 端口且允许 VLAN 100 通过。

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100
[PE1-GigabitEthernet1/0/2] quit
```

### (2) 配置 PE 2

# 配置端口 GigabitEthernet1/0/1 为 Trunk 端口且允许 VLAN 100 通过。

```
<PE2> system-view
[PE2] interface gigabitethernet 1/0/1
[PE2-GigabitEthernet1/0/1] port link-type trunk
[PE2-GigabitEthernet1/0/1] port trunk permit vlan 100
[PE2-GigabitEthernet1/0/1] quit
```

# 配置端口 GigabitEthernet1/0/2 为 Trunk 端口且允许 VLAN 100 通过。

```
[PE2] interface gigabitethernet 1/0/2
[PE2-GigabitEthernet1/0/2] port link-type trunk
```

```
[PE2-GigabitEthernet1/0/2] port trunk permit vlan 100
[PE2-GigabitEthernet1/0/2] quit
```

### (3) 配置 PE 3

# 配置端口 GigabitEthernet1/0/1 为 Trunk 端口且允许 VLAN 100 和 200 通过。

```
<PE3> system-view
[PE3] interface gigabitethernet 1/0/1
[PE3-GigabitEthernet1/0/1] port link-type trunk
[PE3-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

# 在端口 GigabitEthernet1/0/1 上配置 2:2 VLAN 映射，将外层 VLAN 为 100、内层 VLAN 为 5 的报文的 VLAN ID 转换为外层 VLAN 为 200、内层 VLAN 为 6。

```
[PE3-GigabitEthernet1/0/1] vlan mapping tunnel 100 5 translated-vlan 200 6
[PE3-GigabitEthernet1/0/1] quit
```

# 配置端口 GigabitEthernet1/0/2 为 Trunk 端口且允许 VLAN 200 通过。

```
[PE3] interface gigabitethernet 1/0/2
[PE3-GigabitEthernet1/0/2] port link-type trunk
[PE3-GigabitEthernet1/0/2] port trunk permit vlan 200
[PE3-GigabitEthernet1/0/2] quit
```

### (4) 配置 PE 4

# 配置上行端口 GigabitEthernet1/0/1 为 Trunk 端口且允许 VLAN 200 通过。

```
<PE4> system-view
[PE4] interface gigabitethernet 1/0/1
[PE4-GigabitEthernet1/0/1] port link-type trunk
[PE4-GigabitEthernet1/0/1] port trunk permit vlan 200
[PE4-GigabitEthernet1/0/1] quit
```

# 配置下行端口 GigabitEthernet1/0/2 为 Hybrid 端口且允许 VLAN 6 的报文携带 VLAN Tag 通过，允许 VLAN 200 的报文不携带 VLAN Tag 通过。

```
[PE4] interface gigabitethernet 1/0/2
[PE4-GigabitEthernet1/0/2] port link-type hybrid
[PE4-GigabitEthernet1/0/2] port hybrid vlan 6 tagged
[PE4-GigabitEthernet1/0/2] port hybrid vlan 200 untagged
```

# 在端口 GigabitEthernet1/0/2 上配置 1:2 VLAN 映射，为 VLAN 6 的报文添加 VLAN 200 的外层 VLAN Tag。

```
[PE4-GigabitEthernet1/0/2] vlan mapping nest single 6 nested-vlan 200
[PE4-GigabitEthernet1/0/2] quit
```

## 4. 验证配置

### (1) 查看 PE 1 上的 VLAN 映射配置信息

```
[PE1] display vlan mapping
Interface GigabitEthernet1/0/1:
  Outer VLAN   Inner VLAN   Translated Outer VLAN   Translated Inner VLAN
  5             N/A         100                     5
```

### (2) 查看 PE 3 上的 VLAN 映射配置信息

```
[PE3] display vlan mapping
Interface GigabitEthernet1/0/1:
  Outer VLAN   Inner VLAN   Translated Outer VLAN   Translated Inner VLAN
  100          5           200                     6
```

(3) 查看 PE 4 上的 VLAN 映射配置信息

```
[PE4] display vlan mapping
```

```
Interface GigabitEthernet1/0/2:
```

Outer VLAN	Inner VLAN	Translated Outer VLAN	Translated Inner VLAN
6	N/A	200	6

以上信息表明，PE 1 和 PE 4 上的 1:2 VLAN 映射，以及 PE 3 上的 2:2 VLAN 映射配置成功。