项目 3　基于 802.1Q 实现跨交换机环境中部门计算机的互联与隔离

项目描述

某公司现在有财务部和技术部，出于对数据安全的考虑，需要将各部门的计算机隔离。公司的办公地点有两层楼，各部门的计算机通过两台 9 口二层交换机进行互联，两台交换机均通过 G 0/8 端口互联。

本项目的网络拓扑图如图 3-1 所示。

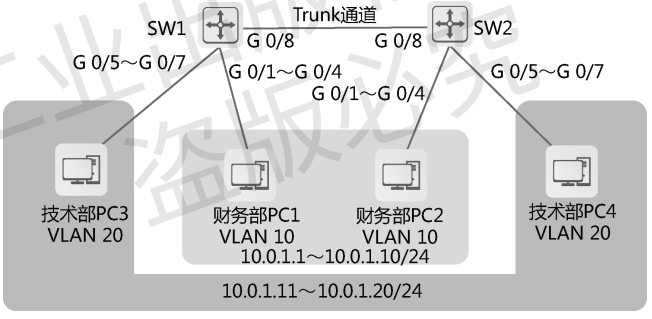

图 3-1　本项目的网络拓扑图

本项目的具体要求如下。

财务部和技术部在这两层楼均有员工办公，其中，财务部的计算机使用交换机 SW1 的 G 0/1～G 0/4 端口及交换机 SW2 的 G 0/1～G 0/4 端口；技术部的计算机使用交换机 SW1 的 G 0/5～G 0/7 端口及交换机 SW2 的 G 0/5～G 0/7 端口。

出于对数据安全的考虑，需要在交换机中为各部门创建相应的 VLAN，用于实现部门内的跨交换机通信，同时避免部门之间互相通信。

所有计算机均采用 10.0.1.0/24 网段，各部门计算机的 IP 地址和接入交换机的端口信息可以参考本项目的网络拓扑图。

相关知识

3.1　VLAN 在实际网络中的应用

网络管理员可以使用不同的方法，将交换机上的端口划分到相应的 VLAN 中，从而在逻辑上分隔广播域。交换机可以使用 VLAN 技术为网络带来以下变化。

- 增加网络中广播域的数量，同时缩小每个广播域的规模，相对地减少每个广播域中终端设备的数量。
- 提高网络设计的逻辑性，网络管理员可以规避地理、物理等因素对网络设计的限制。

在常见的企业园区网设计中，公司会为每个部门都创建一个 VLAN，使其各自形成一个广播域，确保部门内部的员工之间可以通过二层交换机直接进行通信，不同部门的员工之间必须通过三层 IP 路由功能才可以互相通信。企业跨地域 VLAN 的配置应用示例如图 3-2 所示。在图 3-2 中，通过对两栋楼的互联交换机进行配置，可以为财务部创建 VLAN 10、为技术部创建 VLAN 20，不仅实现了部门之间的二层广播隔离，还实现了部门跨交换机的二层通信。

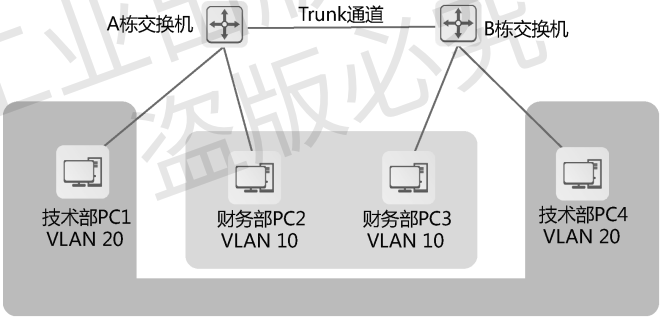

图 3-2　企业跨地域 VLAN 的配置应用示例

3.2　交换机端口的分类

锐捷交换机端口的类型主要有 3 种：Access（接入）、Trunk（干道）和 Hybrid（混合）。

1. Access 端口

Access 是锐捷交换机端口的默认类型。Access 端口主要用于连接计算机等终端设备，只能属于一个 VLAN，也就是只能传输一个 VLAN 中的数据。

Access 端口在收到入站数据帧后，会判断该数据帧中是否携带 VLAN 标签，如果不携带，则将本端口的 VLAN ID 插入该数据帧并进行下一步处理；如果携带，则判断该数据帧中的 VLAN ID 是否与本端口的 VLAN ID 相同，如果相同，则进行下一步处理，否则将该数据帧丢弃。

Access 端口在发送出站数据帧前，会判断这个要被转发的数据帧中携带的 VLAN ID 是否与出站端口的 VLAN ID 相同，如果相同，则去掉 VLAN 标签并进行转发，否则将该数据帧丢弃。

2. Trunk 端口

Trunk 端口主要用于连接交换机等网络设备，它允许传输多个 VLAN 中的数据。

Trunk 端口在接收入站数据帧后，会判断该数据帧中是否携带 VLAN 标签，如果不携带，则将该数据帧插入本端口的 VLAN 并进行下一步处理；如果携带，则判断本端口是否允许传输该数据帧中的 VLAN ID，如果允许，则进行下一步处理，否则将该数据帧丢弃。

Trunk 端口在发送出站数据帧前，会判断这个要被转发的数据帧中携带的 VLAN ID 是否与出站端口的 VLAN ID 相同，如果相同，则去掉 VLAN 标签并进行转发；如果不同，则判断本端口是否允许传输该数据帧中的 VLAN ID，如果允许，则保留原 VLAN 标签并进行转发，否则该将数据帧丢弃。

3. Hybrid 端口

Hybrid 端口可以接收和发送多个 VLAN 中的数据帧，可以连接交换机之间的链路，也可以连接终端设备。

Hybrid 端口在接收入站数据帧后，其处理方法与 Trunk 端口接收入站数据帧后的处理方法相同。

Hybrid 端口在发送出站数据帧前，会判断本端口是否允许传输该数据帧中的 VLAN ID，如果不允许，则将该数据帧丢弃，否则默认按原有的数据帧格式进行转发。

此外，Hybrid 端口还支持以携带 VLAN 标签或不携带 VLAN 标签的方式发送指定 VLAN 中的数据（使用命令“switchport hybrid allowed vlan add tagged vlan”和“switchport hybrid allowed vlan add untagged vlan”进行配置）。

因此，Hybrid 端口兼具 Access 端口和 Trunk 端口的特征，在实际应用中，可以根据对端端口的类型自动适配工作。

项目规划

为了实现各部门之间的隔离，需要在交换机上创建 VLAN，并且将各部门计算机的端口划分到相应的 VLAN 中（将财务部计算机的端口划分到 VLAN 10 中，将技术部计算机的端口划分到 VLAN 20 中）。此外，因为同一个 VLAN 中的计算机分属在不同的交换机上，所以应该将级联通道的端口类型配置为 Trunk，使其可以传输不同 VLAN 中的数据帧。

因此，本项目需要工程师熟悉交换机的 VLAN 创建、端口类型的转换及计算机的 IP 地址配置，主要涉及以下工作任务。

（1）创建 VLAN 并将端口划分到相应的 VLAN 中。

（2）将交换机的互联端口配置为 Trunk 端口，并且允许相应的 VLAN 通过。

（3）配置各部门计算机的 IP 地址，使相同部门的计算机之间可以互相通信。

本项目的 VLAN 规划表如表 3-1 所示，端口规划表如表 3-2 所示，IP 地址规划表如表 3-3 所示。

表 3-1　本项目的 VLAN 规划表

VLAN ID	IP 地址段	用途
VLAN 10	10.0.1.1～10.0.1.10/24	财务部
VLAN 20	10.0.1.11～10.0.1.20/24	技术部

表 3-2 本项目的端口规划表

本端设备	本端端口	端口类型	所属 VLAN	对端设备	对端端口
SW1	G 0/1～G 0/4	Access	VLAN 10	财务部 PC1	—
SW1	G 0/5～G 0/7	Access	VLAN 20	技术部 PC3	—
SW1	G 0/8	Trunk	—	SW2	G 0/8
SW2	G 0/1～G 0/4	Access	VLAN 10	财务部 PC2	—
SW2	G 0/5～G 0/7	Access	VLAN 20	技术部 PC4	—
SW2	G 0/8	Trunk	—	SW1	G 0/8

表 3-3　本项目的 IP 地址规划表

设备	IP 地址
财务部 PC1	10.0.1.1/24
财务部 PC2	10.0.1.5/24
技术部 PC3	10.0.1.11/24
技术部 PC4	10.0.1.15/24

项目实施

任务 3-1　创建 VLAN 并将端口划分到相应的 VLAN 中

► 任务描述

根据本项目中的 VLAN 规划表，首先在交换机上为各部门创建相应的 VLAN 并配置 VLAN 的名称，然后将连接计算机的端口类型转换为 Access，最后配置端口的 VLAN，将端口划分到相应的 VLAN 中。

► 任务实施

（1）在交换机 SW1 上创建 VLAN 并配置 VLAN 的名称。

在交换机上创建 VLAN 后，执行命令“name *name*”，配置 VLAN 的名称，以便记忆，配置命令如下。

```
Ruijie>enable                                    //进入特权模式
Ruijie#config                                    //进入全局模式
Ruijie(config)#hostname SW1                      //将交换机名称修改为 SW1
SW1(config)#vlan 10                              //创建 VLAN 10
SW1(config-vlan)# name Fiance                    //配置 VLAN 10 的名称为 Fiance
SW1(config-vlan)#exit
SW1(config)#vlan 20
SW1(config-vlan)# name Technical
```

（2）在交换机 SW1 上将各部门计算机使用的端口按照部门分别组成批量端口，统一将端口类型转换为 Access，配置端口的 VLAN，将端口划分到相应的 VLAN 中，配置命令如下。

```
SW1(config)#interface range gigabitEthernet 0/1-4 //批量进入端口 G 0/1～G 0/4
SW1(config-if-range)#switchport mode access //将端口类型转换为 Access
SW1(config-if-range)#switchport access vlan 10 //配置端口的默认 VLAN 为 VLAN 10
SW1(config-if-VLAN 10)#exit
SW1(config)#interface range gigabitEthernet 0/5-7
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 20
SW1(config-if-VLAN 20)#exit
```

（3）在交换机 SW2 上创建 VLAN 并配置 VLAN 的名称，配置命令如下。

```
Ruijie>enable
Ruijie#config
Ruijie(config)#hostname SW2
SW2(config)#vlan 10
SW2(config-vlan)#exit
SW2(config)#interface vlan 10
SW2(config-if-VLAN 10)#name Fiance
SW2(config-if-VLAN 10)#exit
SW2(config)#vlan 20
SW2(config)# interface vlan 20
SW2(config-if-VLAN 20)#name Technical
```

（4）在交换机 SW2 上将各部门计算机使用的端口按照部门分别组成批量端口，统一将端口类型转换为 Access，配置端口的 VLAN，将端口划分到相应的 VLAN 中，配置命令如下。

```
SW2(config)#interface range gigabitEthernet 0/1-4
SW2(config-if-range)#switchport mode access
SW2(config-if-range)# switchport access vlan 10
SW2(config-if-range)#exit
SW2(config)#interface range gigabitEthernet 0/5-7
SW2(config-if-range)#switchport mode access
```

```
SW2(config-if-range)# switchport access vlan 20
SW2(config-if-range)#exit
```

► 任务验证

（1）在交换机 SW1 上执行命令“show interfaces switchport”，检查 VLAN 和端口的配置信息，配置命令如下。

```
SW1(config)#show interfaces switchport
Interface           Switchport  Mode   Access  Native  Protected  VLAN lists
------------------- ---------- ------ ------ ------- ---------- --------
GigabitEthernet 0/0  enabled    ACCESS  1       1       Disabled   ALL
GigabitEthernet 0/1  enabled    ACCESS  10      1       Disabled   ALL
GigabitEthernet 0/2  enabled    ACCESS  10      1       Disabled   ALL
GigabitEthernet 0/3  enabled    ACCESS  10      1       Disabled   ALL
GigabitEthernet 0/4  enabled    ACCESS  10      1       Disabled   ALL
GigabitEthernet 0/5  enabled    ACCESS  20      1       Disabled   ALL
GigabitEthernet 0/6  enabled    ACCESS  20      1       Disabled   ALL
GigabitEthernet 0/7  enabled    ACCESS  20      1       Disabled   ALL
GigabitEthernet 0/8  enabled    ACCESS  1       1       Disabled   ALL
```

（2）在交换机 SW2 上执行命令“show interfaces switchport”，检查 VLAN 和端口的配置信息，配置命令如下。

```
SW2(config)#show interfaces switchport
Interface           Switchport  Mode   Access  Native  Protected  VLAN lists
------------------- ---------- ------ ------ ------- ---------- --------
GigabitEthernet 0/0  enabled    ACCESS  1       1       Disabled   ALL
GigabitEthernet 0/1  enabled    ACCESS  10      1       Disabled   ALL
GigabitEthernet 0/2  enabled    ACCESS  10      1       Disabled   ALL
GigabitEthernet 0/3  enabled    ACCESS  10      1       Disabled   ALL
GigabitEthernet 0/4  enabled    ACCESS  10      1       Disabled   ALL
GigabitEthernet 0/5  enabled    ACCESS  20      1       Disabled   ALL
GigabitEthernet 0/6  enabled    ACCESS  20      1       Disabled   ALL
GigabitEthernet 0/7  enabled    ACCESS  20      1       Disabled   ALL
GigabitEthernet 0/8  enabled    ACCESS  1       1       Disabled   ALL
```


任务 3-2　将交换机的互联端口配置为 Trunk 端口

► 任务描述

根据本项目中的 VLAN 规划表，将交换机的互联端口配置为 Trunk 端口，并且允许相应的 VLAN 通过。

► 任务实施

（1）在交换机 SW1 上，将 G 0/8 端口配置为 Trunk 端口，并且允许 VLAN 10 和 VLAN 20 通过。

在交换机上创建 VLAN 后，网络管理员可以进入相应的端口，执行命令“switchport mode {access | trunk | hybrid | uplink}”，修改相应端口的类型，本任务要将端口类型配置为 Trunk；然后执行命令“switchport trunk allowed vlan only {*vlan-id*1 [,*vlan-id*2]}”，配置 Trunk 端口允许哪些 VLAN 通过，本任务允许 VLAN 10 和 VLAN 20 通过。具体的配置命令如下。

```
SW1(config)#interface  gigabitEthernet 0/8
SW1(config-if-GigabitEthernet 0/8)#switchport mode trunk
                          //将端口类型修改为 Trunk
SW1(config-if-GigabitEthernet  0/8)#switchport  trunk  allowed  vlan  only
10,20                     //Trunk 端口只允许在 VLAN 列表中添加 VLAN 10 和 VLAN 20
```

（2）在交换机 SW2 上，将 G 0/8 端口配置为 Trunk 端口，并且允许 VLAN 10 和 VLAN 20 通过，配置命令如下。

```
SW2(config)#interface gigabitEthernet 0/8
SW2(config-if-GigabitEthernet 0/8)#switchport mode trunk
SW2(config-if-GigabitEthernet  0/8)#switchport  trunk  allowed  vlan  only
10,20
```

► 任务验证

（1）在交换机 SW1 上执行命令“show interfaces switchport”，检查 G 0/8 端口的配置信息，配置命令如下。

```
SW1(config-if-GigabitEthernet 0/8)#show interfaces switchport
Interface           Switchport  Mode   Access  Native  Protected  VLAN lists
------------------- ----------  ------ ------ ------- ---------- --------
GigabitEthernet 0/0  enabled    ACCESS  1       1       Disabled   ALL
GigabitEthernet 0/1  enabled    ACCESS  10      1       Disabled   ALL
GigabitEthernet 0/2  enabled    ACCESS  10      1       Disabled   ALL
GigabitEthernet 0/3  enabled    ACCESS  10      1       Disabled   ALL
GigabitEthernet 0/4  enabled    ACCESS  10      1       Disabled   ALL
GigabitEthernet 0/5  enabled    ACCESS  20      1       Disabled   ALL
GigabitEthernet 0/6  enabled    ACCESS  20      1       Disabled   ALL
GigabitEthernet 0/7  enabled    ACCESS  20      1       Disabled   ALL
GigabitEthernet 0/8  enabled    TRUNK   1       1       Disabled   10,20
```

可以看到，G 0/8 端口的类型为 Trunk，并且在 VLAN lists 中添加了 VLAN 10、VLAN 20。

（2）在交换机 SW2 上执行命令“show interfaces switchport”，检查 G 0/8 端口的配置信

息，配置命令如下。

```
SW2(config-if-GigabitEthernet 0/8)#show interfaces switchport
Interface           Switchport  Mode   Access  Native  Protected  VLAN lists
------------------- ----------- ------ ------ ------- ---------- --------
GigabitEthernet 0/0  enabled    ACCESS  1       1       Disabled   ALL
GigabitEthernet 0/1  enabled    ACCESS  10      1       Disabled   ALL
GigabitEthernet 0/2  enabled    ACCESS  10      1       Disabled   ALL
GigabitEthernet 0/3  enabled    ACCESS  10      1       Disabled   ALL
GigabitEthernet 0/4  enabled    ACCESS  10      1       Disabled   ALL
GigabitEthernet 0/5  enabled    ACCESS  20      1       Disabled   ALL
GigabitEthernet 0/6  enabled    ACCESS  20      1       Disabled   ALL
GigabitEthernet 0/7  enabled    ACCESS  20      1       Disabled   ALL
GigabitEthernet 0/8  enabled    TRUNK   1       1       Disabled   10,20
```

可以看到，G 0/8 端口的类型为 Trunk，并且在 VLAN lists 中添加了 VLAN 10、VLAN 20。

任务 3-3　配置各部门计算机的 IP 地址

► 任务描述

根据本项目的 IP 地址规划表，为各部门的计算机配置 IP 地址，使相同部门的计算机之间可以互相通信。

► 任务实施

财务部 PC1 的 IP 地址配置如图 3-3 所示，同理，完成其他计算机的 IP 地址配置。

图 3-3　财务部 PC1 的 IP 地址配置

► 任务验证

（1）在财务部 PC1 上执行命令“ipconfig”，查看其 IP 地址的配置信息，配置命令如下。

```
C:\Users\Administrator>ipconfig     //显示本机 IP 地址的配置信息

本地连接:

   连接特定的 DNS 后缀 . . . . . . . . . . . . . . . :
   IPv4 地址 . . . . . . . . . . . . . . . . . . . . . . . : 10.0.1.1(首选)
   子网掩码 . . . . . . . . . . . . . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . . . . . . . . . . . . . :
```

结果显示，财务部 PC1 的 IP 地址配置正确。

（2）在其他计算机上执行命令“ipconfig”，验证其 IP 地址配置是否正确。

项目验证

（1）使用 Ping 命令测试各部门内部计算机之间的通信情况。

使用财务部 PC1 Ping 财务部 PC2，配置命令如下。

```
C:\Users\Administrator>ping 10.0.1.5

正在 Ping 10.0.1.5 具有 32 字节的数据:
来自 10.0.1.5 的回复: 字节=32 时间=1ms TTL=64
来自 10.0.1.5 的回复: 字节=32 时间=5ms TTL=64
来自 10.0.1.5 的回复: 字节=32 时间=1ms TTL=64
来自 10.0.1.5 的回复: 字节=32 时间=1ms TTL=64

10.0.1.5 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms，最长 = 5ms，平均 = 2ms
```

可以看出，在将端口加入不同的 VLAN 后，相同 VLAN 中的计算机之间可以互相通信。

（2）使用 Ping 命令测试不同部门计算机之间的通信情况。

使用财务部 PC1 Ping 技术部 PC3，配置命令如下。

```
C:\Users\Administrator>ping 10.0.1.11

正在 Ping 10.0.1.11 具有 32 字节的数据:
来自 10.0.1.1 的回复: 无法访问目标主机。
```

```
来自 10.0.1.1 的回复：无法访问目标主机。
来自 10.0.1.1 的回复：无法访问目标主机。
来自 10.0.1.1 的回复：无法访问目标主机。

10.0.1.11 的 Ping 统计信息：
    数据包：已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
```

可以看出，在将端口加入不同的 VLAN 后，不同 VLAN 中的计算机之间不可以互相通信。

项目拓展

一、理论题

1.（多选）锐捷以太网交换机端口的类型主要有（　　）。

A．Access　　B．Hybrid　　C．Trunk　　D．QinQ

2．在交换机的端口下执行命令“switchport trunk allowed vlan all”的作用是（　　）。

A．与该端口相连的对端端口必须同时配置命令“switchport trunk allowed vlan all”

B．该端口允许所有 VLAN 的数据帧通过

C．相连的对端设备可以动态确定允许哪些 VLAN ID 通过

D．如果为相连的远端设备配置了“switchport access vlan 3”，那么两台设备之间的 VLAN 3 无法互通

3．关于交换机能够通过 VLAN 技术为网络带来的变化，以下说法错误的是（　　）。

A．增加了网络中广播域的数量，同时扩大了每个广播域的规模

B．降低了网络设计的逻辑性，网络管理员可以规避地理、物理等因素对网络设计的限制

C．提高了网络设计的逻辑性，网络管理员可以规避地理、物理等因素对网络设计的限制

D．相对地减少了每个广播域中终端设备的数量

4．关于以太网交换机的 Access 端口发送数据帧，以下说法正确的是（　　）。

A．该端口携带 VLAN 标签，VLAN ID 为 1

B．不携带 VLAN 标签

C．携带 VLAN 标签，VLAN ID 为该端口 VLAN 的值

D．携带 VLAN 标签，VLAN ID 为该端口的默认 VLAN 号

5.（多选）一个 Trunk 端口的 VLAN ID 是 10，如果在该端口下执行命令“switchport trunk allowed vlan only 11,12”，那么（　　）的数据帧可以通过该端口进行传输。

A．VLAN 1　　B．VLAN 11

C．VLAN 12　　D．VLAN 10

二、项目实训题

1．实训项目描述

某公司现在有财务部和技术部，出于对数据安全的考虑，需要将各部门的计算机隔离。公司的办公地点有两层楼，各部门的计算机通过两台 9 口二层交换机进行互联，两台交换机均通过 G 0/8 端口互联。

本实训项目的网络拓扑图如图 3-4 所示。

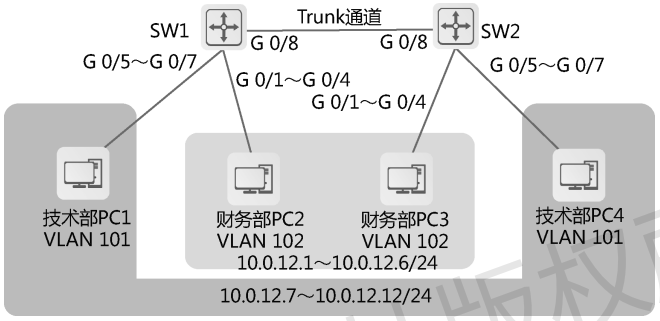

图 3-4　本实训项目的网络拓扑图

2．实训项目规划

根据本实训项目的相关描述和网络拓扑图，完成本实训项目的各个规划表。

（1）完成本实训项目的 VLAN 规划表，如表 3-4 所示。

表 3-4　本实训项目的 VLAN 规划表

VLAN ID	IP 地址段	用途

（2）完成本实训项目的端口规划表，如表 3-5 所示。

表 3-5　本实训项目的端口规划表

本端设备	本端端口	端口类型	所属 VLAN	对端设备	对端端口

（3）完成本实训项目的 IP 地址规划表，如表 3-6 所示。

表 3-6　本实训项目的 IP 地址规划表

设备	IP 地址

续表

设备	IP 地址

3．实训项目要求

（1）根据本实训项目的网络拓扑图及规划表，首先在交换机上为各部门创建相应的 VLAN 并配置 VLAN 的名称，然后将连接计算机的端口类型转换为 Access，最后配置端口的 VLAN，将端口划分到相应的 VLAN 中。

（2）将交换机的互联端口配置为 Trunk 端口，并且允许相应的 VLAN 通过。

（3）根据 IP 地址规划表，为各部门的计算机配置 IP 地址，使各部门的计算机之间可以互相通信。

（4）根据以上要求完成配置，执行以下验证命令，并且截图保存相关结果。

步骤 1：使用 Ping 命令测试各部门内部计算机之间的通信情况，如使用财务部计算机 Ping 本部门的计算机。

步骤 2：使用 Ping 命令测试不同部门计算机之间的通信情况，如使用财务部的计算机 Ping 技术部的计算机。

步骤 3：执行命令“show vlan”，查看 VLAN 的端口划分情况。