项目 3

基于 802.1Q 实现跨交换机环境下的部门计算机互联与隔离

项目描述

某公司现有财务部和技术部两个部门，出于数据安全的考虑，需要将各部门的计算机进行隔离。公司办公地点有两层楼，各部门的计算机通过两台 24 口二层交换机进行互联，这两台交换机均通过 G0/0/1 互联。公司网络拓扑图如图 3-1 所示。项目具体要求如下。

（1）财务部和技术部在这两层楼均有员工办公，其中财务部计算机使用 SW1 的 Eth0/0/1～Eth0/0/5 端口及 SW2 的 Eth0/0/1～Eth0/0/5 端口；技术部计算机使用 SW1 的 Eth0/0/6～Eth0/0/10 端口及 SW2 的 Eth0/0/6～Eth0/0/10 端口。

（2）出于数据安全的考虑，需要在交换机上为各部门创建相应的 VLAN，在实现部门内跨交换机通信的同时避免部门间相互通信。

（3）所有计算机均采用 10.0.1.0/24 网段，各部门的 IP 地址和接入交换机的端口信息如图 3-1 所示。

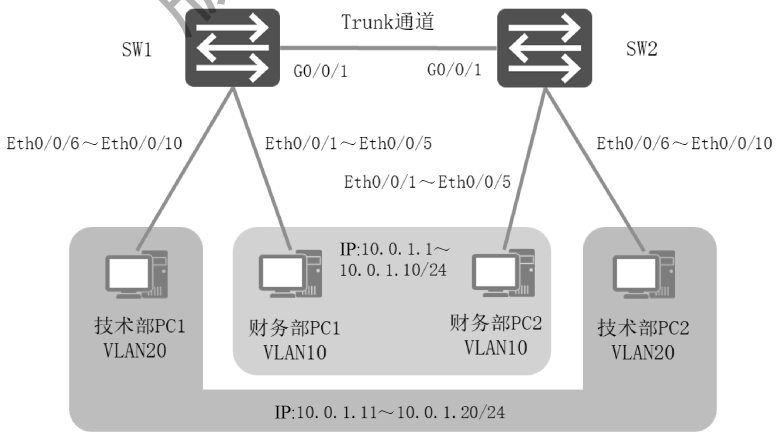

图 3-1　公司网络拓扑图

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把交换机上的每个端口划分到某个 VLAN 中，以此在逻辑上分隔广播域。交换机能够通过 VLAN 技术为网络带来以下变化。

（1）增加了网络中广播域的数量，同时缩小了每个广播域的规模，相对地减少了每个广播域中终端设备的数量。

（2）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。

在常见的企业园区网设计中，公司会为每个部门创建一个 VLAN，每个 VLAN 各自形成一个广播域，部门内部员工之间能够通过二层交换机直接通信，不同部门的员工之间必须通过三层 IP 路由功能才可以相互通信。如图 3-2 所示，通过对两栋楼的互联交换机的配置，可以实现为两栋楼的财务部创建 VLAN10，为技术部创建 VLAN20，不仅实现了部门间的二层广播隔离，而且实现了部门跨交换机的二层通信。

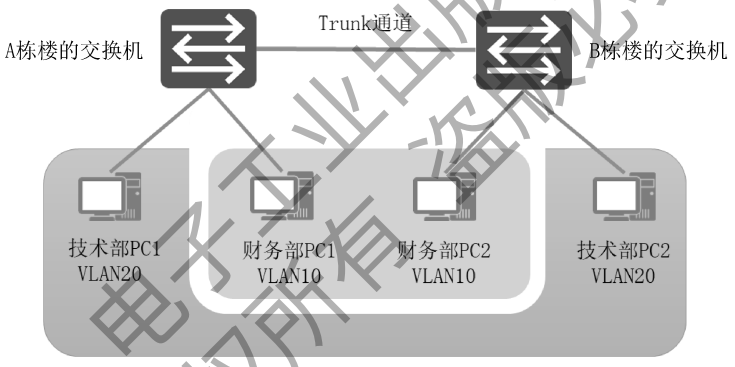

图 3-2　企业跨地域 VLAN 的配置应用

3.2 交换机端口的分类

华为交换机端口的工作模式主要有 3 种：Access（接入）端口、Trunk（干道）端口和 Hybrid（混合）端口。

1．Access 端口

Access 端口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 的数据。

Access 端口收到入站数据帧后，会判断这个数据帧是否携带 VLAN 标签。若不携带，则为数据帧插入本端口的 PVID 并进行下一步处理；若携带，则判断数据帧中携带的 VLAN ID 是否与本端口的 PVID 相同，若相同则进行下一步处理，否则丢弃。

Access 端口在发送出站数据帧之前，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 PVID 相同，若相同则去掉 VLAN 标签进行转发，否则丢弃。

2．Trunk 端口

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

Trunk 端口收到入站数据帧后，会判断这个数据帧是否携带 VLAN 标签。若不携带，则为数据帧插入本端口的 PVID 并进行下一步处理；若携带，则判断本端口是否允许传输这个数据帧的 VLAN ID，若允许则进行下一步处理，否则丢弃。

Trunk 端口在发送出站数据帧之前，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 PVID 相同，若相同则去掉 VLAN 标签进行转发；若不同则判断本端口是否允许传输这个数据帧的 VLAN ID，若允许则转发（保留原标签），否则丢弃。

3．Hybrid 端口

Hybrid 端口是华为系列交换机端口的默认端口类型，它能够接收和发送多个 VLAN 的数据帧，可以用于连接交换机之间的链路，也可以用于连接终端设备。

Hybrid 端口和 Trunk 端口在接收入站数据时，处理方法是相同的。但在发送出站数据时，Hybrid 端口会判断该帧的 VLAN ID 是否允许被通过，若不允许则丢弃，否则默认按原有数据帧格式进行转发。同时，它还支持携带 VLAN 或不携带 VLAN 标签的方式发送指定 VLAN 的数据（使用【port hybrid tagged vlan】命令和【port hybrid untagged vlan】命令进行配置）。

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工作模式自动适配工作。

项目规划设计

为实现各部门之间的隔离，需要在交换机上创建 VLAN，并将各部门计算机的相应端口划分到相应的 VLAN，其中，VLAN10 和 VLAN20 分别用于财务部和技术部。同时，因同一个 VLAN 中的计算机分属在不同的交换机上，故级联的通道应被配置为 Trunk 模式，使其能够传输不同 VLAN 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。本项目涉及以下工作任务。

（1）创建 VLAN 并将端口划分到相应的 VLAN。在交换机上为各部门创建相应的 VLAN 并配置 VLAN 描述，将连接计算机的端口类型转换模式，并将端口划分到相应的 VLAN。

（2）配置交换机互联端口为 Trunk 模式。将交换机互联端口配置为 Trunk 模式并允许相应的 VLAN 通过。

（3）配置计算机的 IP 地址，使各部门的计算机可以相互通信。

VLAN 规划表 1、端口规划表 1 和 IP 地址规划表 1 如表 3-1～表 3-3 所示。

表 3-1　VLAN 规划表 1

VLAN ID	IP 地址段	用途
VLAN10	10.0.1.1～10.0.1.10/24	财务部
VLAN20	10.0.1.11～10.0.1.20/24	技术部

表 3-2　端口规划表 1

本端设备	本端端口	端口类型	所属 VLAN	对端设备	对端端口
SW1	Eth0/0/1～Eth0/0/5	Access	VLAN10	财务部 PC1	—
SW1	Eth0/0/6～Eth0/0/10	Access	VLAN20	技术部 PC1	—
SW1	G0/0/1	Trunk		SW2	G0/0/1
SW2	Eth0/0/1～Eth0/0/5	Access	VLAN10	财务部 PC2	—
SW2	Eth0/0/6～Eth0/0/10	Access	VLAN20	技术部 PC2	—
SW2	G0/0/1	Trunk		SW1	G0/0/1

表 3-3　IP 地址规划表 1

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 PC1	10.0.1.11/24
技术部 PC2	10.0.1.20/24

项目实施

任务 3-1　创建 VLAN 并将端口划分到相应的 VLAN

任务描述

根据表 3-1 在交换机上为各部门创建相应的 VLAN 并配置 VLAN 描述，将连接计算机的端口类型转换为 Access 模式，并将端口划分到相应的 VLAN。

扫一扫，看微课

任务实施

（1）在 SW1 上创建 VLAN 并配置 VLAN 描述。

在交换机上创建 VLAN 后，可以使用【description *name*】命令修改 VLAN 的描述信息，方便记忆，配置命令如下。

```
[Huawei]system-view                  //进入系统视图
[Huawei]sysname SW1                  //将交换机名称更改为 SW1
[SW1]vlan 10                         //创建 VLAN10
[SW1-vlan10]description Fiance       //配置 VLAN10 的描述信息为 Fiance
[SW1]vlan 20
[SW1-vlan20]description Technical
```

（2）在 SW1 上将各部门计算机所使用的端口按部门分别组成端口组，统一将端口类型转换为 Access 模式并设置端口 PVID，将端口划分到相应的 VLAN，配置命令如下。

```
//将端口 Eth0/0/1～Eth0/0/5 组成一个端口组
[SW1]port-group group-member Eth 0/0/1 to Eth0/0/5
[SW1-port-group]port link-type access     //修改端口类型为 Access 模式
[SW1-Ethernet0/0/1]port link-type access
[SW1-Ethernet0/0/2]port link-type access
```

```
[SW1-Ethernet0/0/3]port link-type access
[SW1-Ethernet0/0/4]port link-type access
[SW1-Ethernet0/0/5]port link-type access
[SW1-port-group]port default vlan 10    //配置端口的默认 VALN 为 VLAN10
[SW1-Ethernet0/0/1]port default vlan 10
[SW1-Ethernet0/0/2]port default vlan 10
[SW1-Ethernet0/0/3]port default vlan 10
[SW1-Ethernet0/0/4]port default vlan 10
[SW1-Ethernet0/0/5]port default vlan 10
[SW1-port-group]quit
[SW1]port-group group-member Eth 0/0/6 to Eth 0/0/10
[SW1-port-group]port link-type access
[SW1-Ethernet0/0/6]port link-type access
[SW1-Ethernet0/0/7]port link-type access
[SW1-Ethernet0/0/8]port link-type access
[SW1-Ethernet0/0/9]port link-type access
[SW1-Ethernet0/0/10]port link-type access
[SW1-port-group]port default vlan 20
[SW1-Ethernet0/0/6]port default vlan 20
[SW1-Ethernet0/0/7]port default vlan 20
[SW1-Ethernet0/0/8]port default vlan 20
[SW1-Ethernet0/0/9]port default vlan 20
[SW1-Ethernet0/0/10]port default vlan 20
[SW1-port-group]quit
```

（3）在 SW2 上创建 VLAN 并配置 VLAN 描述，配置命令如下。

```
[Huawei]system-view
[Huawei]sysname SW2
[SW2]vlan 10
[SW2-vlan10]description Fiance
[SW2]vlan 20
[SW2-vlan20]description Technical
```

（4）在 SW2 上将各部门计算机所使用的端口按部门分别组成端口组，统一将端口类型转换为 Access 模式并设置端口 PVID，将端口划分到相应的 VLAN，配置命令如下。

```
[SW2]port-group group-member Eth 0/0/1 to Eth 0/0/5
[SW2-port-group]port link-type access
[SW2-Ethernet0/0/1]port link-type access
[SW2-Ethernet0/0/2]port link-type access
[SW2-Ethernet0/0/3]port link-type access
[SW2-Ethernet0/0/4]port link-type access
[SW2-Ethernet0/0/5]port link-type access
[SW2-port-group]port default vlan 10
[SW2-Ethernet0/0/1]port default vlan 10
[SW2-Ethernet0/0/2]port default vlan 10
[SW2-Ethernet0/0/3]port default vlan 10
[SW2-Ethernet0/0/4]port default vlan 10
[SW2-Ethernet0/0/5]port default vlan 10
[SW2-port-group]quit
[SW2]port-group group-member Eth 0/0/6 to Eth0/0/10
[SW2-port-group]port link-type access
[SW2-Ethernet0/0/6]port link-type access
```

```
[SW2-Ethernet0/0/7]port link-type access
[SW2-Ethernet0/0/8]port link-type access
[SW2-Ethernet0/0/9]port link-type access
[SW2-Ethernet0/0/10]port link-type access
[SW2-port-group]port default vlan 20
[SW2-Ethernet0/0/6]port default vlan 20
[SW2-Ethernet0/0/7]port default vlan 20
[SW2-Ethernet0/0/8]port default vlan 20
[SW2-Ethernet0/0/9]port default vlan 20
[SW2-Ethernet0/0/10]port default vlan 20
[SW2-port-group]quit
```

任务验证

（1）配置完成后，在 SW1 上使用【display port vlan】命令检查 VLAN 和端口配置情况，配置命令如下。

```
[SW1]display port vlan
Port                Link Type    PVID  Trunk VLAN List
--------------------------------------------------------------------------------
Ethernet0/0/1         access      10    -
Ethernet0/0/2         access      10    -
Ethernet0/0/3         access      10    -
Ethernet0/0/4         access      10    -
Ethernet0/0/5         access      10    -
Ethernet0/0/6         access      20    -
Ethernet0/0/7         access      20    -
Ethernet0/0/8         access      20    -
Ethernet0/0/9         access      20    -
Ethernet0/0/10        access      20    -
Ethernet0/0/11        hybrid      1     -
Ethernet0/0/12        hybrid      1     -
省略部分内容……
```

（2）在 SW2 上使用【display port vlan】命令检查 VLAN 和端口配置情况，配置命令如下。

```
[SW2]display port vlan
Port                Link Type    PVID  Trunk VLAN List
--------------------------------------------------------------------------------
Ethernet0/0/1         access      10    -
Ethernet0/0/2         access      10    -
Ethernet0/0/3         access      10    -
Ethernet0/0/4         access      10    -
Ethernet0/0/5         access      10    -
Ethernet0/0/6         access      20    -
Ethernet0/0/7         access      20    -
Ethernet0/0/8         access      20    -
Ethernet0/0/9         access      20    -
Ethernet0/0/10        access      20    -
Ethernet0/0/11        hybrid      1     -
Ethernet0/0/12        hybrid      1     -
省略部分内容……
```

任务 3-2　配置交换机互联端口为 Trunk 模式

任务描述

根据表 3-1 将交换机互联端口配置为 Trunk 端口并允许相应的 VLAN 通过。

任务实施

（1）在 SW1 上配置 G0/0/1 为 Trunk 端口，允许 VLAN10 和 VLAN20 通过。

在交换机上创建 VLAN 后，管理员就可以进入对应端口，使用【port link-type { access | trunk | hybrid }】命令修改对应端口的模式。当将端口配置为 Trunk 端口后，需要使用【port trunk allow-pass vlan { vlan-id1 [to vlan-id2] }】命令配置 Trunk 干道允许哪些 VLAN 通过，配置命令如下。

```
[SW1]interface G0/0/1                                  //进入 G0/0/1 端口
[SW1-GigabitEthernet0/0/1]port link-type trunk   //修改端口类型为 Trunk 模式
//Trunk 允许在 VLAN 列表中添加 VLAN10 和 VLAN20
[SW1-GigabitEthernet0/0/1]port trunk allow-pass vlan 10 20
```

（2）在 SW2 上配置 G0/0/1 为 Trunk 端口，允许 VLAN10 和 VLAN20 通过，配置命令如下。

```
[SW2]interface G0/0/1
[SW2-GigabitEthernet0/0/1]port link-type trunk
[SW2-GigabitEthernet0/0/1]port trunk allow-pass vlan 10 20
```

任务验证

（1）配置完成后，在 SW1 上使用【display port vlan G0/0/1】命令检查 G0/0/1 端口的配置情况，配置命令如下。

```
[SW1]display port vlan G0/0/1
Port               Link Type   PVID  Trunk VLAN List
--------------------------------------------------------------------------------
GigabitEthernet0/0/1   trunk       1    1 10 20
省略部分内容……
```

可以看到，G0/0/1 端口的链路模式为 Trunk，且 Trunk VLAN 列表中添加了 VLAN10 和 VLAN20。

（2）在 SW2 上使用【display port vlan G0/0/1】命令检查 G0/0/1 端口的配置情况，配置命令如下。

```
[SW2]display port vlan G0/0/1
Port                Link Type    PVID  Trunk VLAN List
--------------------------------------------------------------------------------
GigabitEthernet0/0/1    trunk       1    1 10 20
省略部分内容……
```

可以看到，G0/0/1 端口的链路模式为 Trunk，且 Trunk VLAN 列表中添加了 VLAN10 和 VLAN20。

任务 3-3　配置计算机的 IP 地址

任务描述

根据表 3-3 为各计算机配置 IP 地址。

任务实施

（1）根据表 3-3 为各计算机配置 IP 地址。

（2）财务部 PC1 的 IP 地址配置结果如图 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 地址配置结果

任务验证

（1）在财务部 PC1 上使用【ipconfig】命令查看 IP 地址，配置命令如下。

```
PC1>ipconfig     //显示本机的 IP 地址配置信息

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. . . . . . . . . . . . .  :
```

（2）在其他计算机上同样使用【ipconfig】命令查看 IP 地址。

扫一扫，看微课

项目验证

（1）使用【ping】命令测试各部门的内部通信情况。使用财务部计算机 Ping 本部门的计算机，配置命令如下。