7.3 隧道技术与应用案例

企业网络组建和改造项目中，很少有企业只采用一台交换机上实现吧？如果企业规模扩大了，在原来的交换机网络中，如果新添加一台交换机，很可能出来新的问题来，让我们来看看本小节的实际例子。

7.3.1 案例场景描述

某平面广告公司原有 20 多名员工，共有 19 个客户端计算机接入了公司的交换机。广告公司公司规模较小，并且没有配网络管理员，公司的网络由集成商组建后一直比较稳定的运行着。由于业务的拓展，公司从平面广告业务发展到影视制作等多种媒介资源的为一体的企业。各个部门都招聘了员工，人员从 20 多名增加到 40 多名，客户端计算机的数量也翻了一倍，原有的 24 口交换机已经不能满足现在的需求。

公司新购置了一台 24 口交换机，一位网络技术相对较好的老员工被安排负责此项工作。这位老兄在之前的网络集成时就负责本公司和集成商的配合工作，此次他按照原来留下的配置文档再新交换机上也敲了一遍。

第 1 步：创建 VLAN

```
Switch2#vlan database
Switch2(vlan)#vlan 2 name meijie      //建立媒介部 VLAN
Switch2(vlan)#vlan 3 name shangwu   //建立商务部 VLAN
Switch2(vlan)#vlan 4 name caiwu       //建立财务部 VLAN
```

第 2 步：把端口分配到 VLAN

```
Switch2(config)#interface range fastEthernet 0/5 - 8
Switch2(config-if)#Switchport access vlan 2  //将 5 至 8 端口放入 VLAN2 中
Switch2(config)#interface range fastEthernet 0/9 - 11
Switch2(config-if)#Switchport access vlan 3        //9 至 11 端口放入 VLAN3 中
…后续步骤省略
```

应该注意，interface range fastEthernet X/X - X 是应用在 Cisco IOS 软件 12.1 以上的版本，如果你使用的是 Cisco IOS 软件 12.1 以前的发布的版本的话，应该用命令：Switchport access vlan vlanID，把端口加入 VLAN。

完成上述步骤后，将所有客户端从配线架上用跳线接入到交换机的不同端口，并用一条跳线连接了 Switch1 的 fastEthernet 0/2 和 Switch2 的 fastEthernet 0/1 端口。本以为这项工作就这样顺利完成了，但不同交换机中同一部门的客户端就是无法通信。

起初以为是 IP 地址配置的问题，但检查客户端之后，发现同一台交换机中（同一 VLAN）的客户端通信一点问题也没有。在尝试了一切可能的办法之后，还无法解决问题，所以只能求助原理负责系统集成那家公司前来帮忙。

工程师到达广告公司之后，首先在新交换机上检查了 VLAN 的配置，发现 VLAN 的配置没有问题。在特权模式下使用命令用 show vlan 来检查是否将端口分配给正确的 VLAN：

```
VLAN  Name                Status    Ports
====  ================  ======  ========================
1       default               active   Fa0/2, Fa0/4, Fa0/16, Fa0/17
                                        Fa0/18, Fa0/19, Fa0/20,
```

```
                                          Fa0/22, Fa0/23, Fa0/24,
                                          Gi0/1                Gi0/2
2     meijie                    active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
3     shangwu                   active    Fa0/9, Fa0/10, Fa0/11
4     caiwu                     active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
1002  fddi-default              active
1003  token-ring-default        active
1004  fddinet-default           active
1005  trnet-default             active
```

既然已经分配了正确的 VLAN 名称和接口，为什么在两台交换机之间无法通信呢？要得出新交换机的客户端和原有交换机不能通信的真正原因，还要从 VLAN 工作的原理中找出答案。

7.3.2　Trunking 技术的实现

在“7.1.2 VLAN 的实现原理”部分看到，要传输多个 VLAN 的通信，就需要用专门的协议封装或者加上标记（tag），以便接收设备能区分数据所属的 VLAN。VLAN 标识从逻辑上定义了，数据包使用哪种协议进行封装。而最常用到的是 IEEE 802.1Q 和 CISCO 私有的 ISL 协议。

除 IEEE 802.1Q、ISL 协议外还有两种封装技术：IEEE 802.10 和 ATM LAN 仿真（LANE）。IEEE 802.10 常用于光纤分布接口（FDDI）帧内传达 VLAN 的信息。而 LANE 则用于异步传输模式（ATM）网络中传输 VLAN。下面介绍 IEEE 802.1Q 和 ISL 协议，以替代 ISL 的动态中继协议。

1．ISL（交换机间链路）

是一种 CISCO 专用的协议，用于连接多个 CISCO 交换机。使用 ISL 后，每个数据帧头部都会被附加 26 字节的“ISL 包头（ISL Header）”，并且在帧尾携带上包括 ISL 包头在内的整个数据帧进行计算后得到的 4 字节 CRC 值。换而言之，就是总共增加了 30 字节的信息，如图 7-5 所示。在使用 ISL 的环境下，当数据帧离开汇聚链路时，只要简单地去除 ISL 包头和新 CRC 就可以了。由于原先的数据帧及其 CRC 都被完整保留，因此无须重新计算 CRC。ISL 有如用 ISL 包头和新 CRC 将原数据帧整个包裹起来，因此也被称为“封装型 VLAN（Encapsulated VLAN）”。图 7-8 中显示了 ISL 的数据帧。

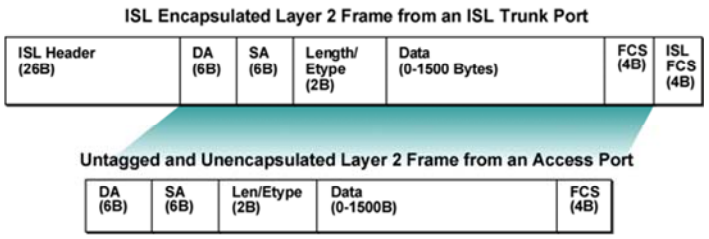

图 7-8　ISL 的数据帧

2．IEEE 802.1Q（虚拟桥接局域网标准）

IEEE 802.1Q，俗称“Dot One Q”，正式名称是虚拟桥接局域网标准，用在不同的产家生产的交换机之间。一个 IEEE 802.1Q 干道端口同时支持加标签和未加标签的流量。一个 802.1Q 干道端口被指派了一个默认的端口 Vlan ID（PVID），并且所有的未加标签的流量在该端口的

默认 PVID 上传输。一个带有和外出端口的默认 PVID 相等的 Vlan ID 的包发送时不被加标签。所有其他的流量发送是被加上 Vlan 标签的。

IEEE 802.1Q 所附加的 VLAN 识别信息，位于数据帧中“发送源 MAC 地址”与“类别域（Type Field）”之间。具体内容为 2 字节的 TPID 和 2 字节的 TCI，共计 4 字节。在数据帧中添加了 4 字节的内容，那么 CRC 值自然也会有所变化。这时数据帧上的 CRC 是插入 TPID、TCI 后，对包括它们在内的整个数据帧重新计算后所得的值。

而当数据帧离开汇聚链路时，TPID 和 TCI 会被去除，这时还会进行一次 CRC 的重新计算。TPID 的值，固定为 0x8100。交换机通过 TPID，来确定数据帧内附加了基于 IEEE 802.1Q 的 VLAN 信息。基于 IEEE 802.1Q 附加的 VLAN 信息，就像在传递物品时附加的标签。因此，它也被称作“标签型 VLAN（Tagging VLAN）”。图 7-9 中显示了 IEEE 802.1Q 的数据包。

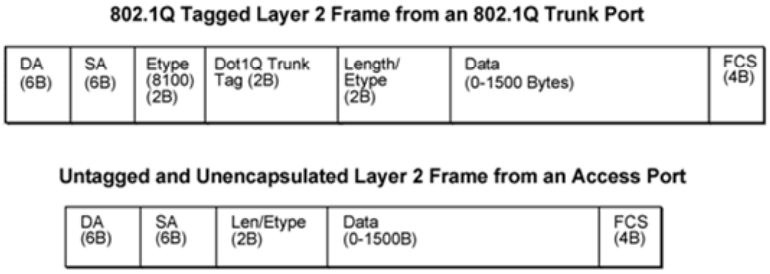

图 7-9　IEEE 802.1Q 的数据帧

不论是 IEEE 802.1Q 的“Tagging VLAN”，还是 ISL 的“Encapsulated VLAN”，都不是很严密的称谓。不同的书籍与参考资料中，上述词语有可能被混合使用，因此需要大家在学习时格外注意。

3．动态中继协议

动态中继协议 DTP，是 VLAN 组中思科的私有协议，主要用于协商两台设备间链路上的中继过程及中继封装 802.1Q 类型。DTP 的用途是取代动态 ISL（Dynamic ISL，DISL）。

下列是 DTP 可以配置的几种不同的状态：

- Access：使某个接口无条件进入 Access 模式，无 DTP 功能。
- Trunk：使某个接口无条件进入 trunk 模式并进行 trunk 链路协商，无论其邻居接口处于何种模式。
- Nonegotiate：指定 DTP 协商报文不允许在二层接口上发送。非协商状态，使接口成为永久的中继接口。由于接口不使用 DTP 信息帧进行通信，因此不会有协商发生。如果与非交换机设备相连的交换机接口存在 DTP 问题，那么在使用 trunk 之后可以使用 nonegotiate，使得接口可以继续中继，但不会发送任何 DTP 信息。
- Dynamic desirable：使某个接口既主动发送 DTP 报文，也允许对 DTP 报文进行响应，这是以太网接口的默认状态。如果邻居接口是中继接口，并且被设置为 on，desirable 或 auto，那么希望 desirable 状态下的这个接口成为中继接口。
- Dynamic auto：使某个接口可以响应 DTP 报文，但不允许主动发送 DTP 报文。只有在相邻接口要求该接口成为中继接口时才会成为中继接口。这是所有交换机接口的默认配置。auto 接口不会主动要求对方，如果两个接口都被配置成 auto 状态，那么

这两个接口都不会成为中继端。

- On：无论对端配置如何，该接口始终为中继接口。使用 on 状态时，必须指明帧的标记方式，因为此状态下接口不与对端进行协商。
- Off：该拉口永远是非中继接口。

7.3.3　隧道技术的用途

在前面已经出现了很多次 Trunk 这个词汇，但并没有详细的进行解答。我们知道交换机的接口可以运行在接入模式（Access Mode）或者干道模式（Trunk Mode）。交换机接口所连接的链路也被相应地称为接入链路和 trunk 链路。在接入模式下，接口属于且仅属于一个 VLAN。

而 Trunk（干道）是一种封装技术，它是一条点到点的链路，主要功能就是仅通过一条链路就可以连接多个交换机从而扩展已配置的多个 VLAN，如图 7-10 所示。

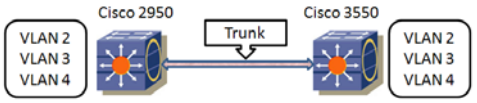

图 7-10　实现不同交换机上同个 VLAN 的通信

同时 trunk 链路可以连接一台交换机或者路由器或者服务器（特殊网卡），还可以采用通过 trunk 技术和上级交换机级联的方式来扩展接口的数量，可以达到近似堆叠的功能，节省了网络硬件的成本。

trunk 链路不属于任何一个 VLAN，它只是在网络中起到了管道的作用。Trunk 承载的 VLAN 范围，默认下是 1～1005，可以修改，但必须有 1 个 Trunk 协议。使用 Trunk 时，两台交换机连接接口上的协议要一致。配置为 Trunk 链路的接口，通常都是交换机上支持最大带宽的带宽口。

表 7-6 列出了和 Trunk 操作有关的命令。

表 7-6　在基于 IOS 的交换机上配置 trunk

步　骤	命　令	解　释
1	Switch#configure terminal	进入全局配置模式
2	Switch(config)# interface interface-id	进入要分配的接口
3	Switch(config-if)#switchport mode trunk	将端口设置为 trunk 模式
3（1）	Switch(config-if)#switchport mode dynamic desirable	在仅支持 802.1Q 封装，但支持 DTP 功能的交换机上主动尝试转换为 trunk 模式
3（2）	Switch(config-if)#switchport mode dynamic auto	在仅支持 802.1Q 封装，但支持 DTP 功能的交换机上转换为 trunk 模式，由邻居接口决定
3（3）	Switch(config-if)#switchport nonegotiate	在仅支持 802.1Q 封装，但支持 DTP 功能的交换机上将接口永久设置为 trunk 模式，但禁止产生 DTP 帧
4	Switch(config-if)#switchport trunk encapsulation {isl | dot1q}	配置接口是使用 ISL 或者 802.1Q 封装，两端链路必须采用相同的封装格式
5	Switch(config-if)#switchport trunk allowed vlan remove vlan-list	要限制 trunk 传送的 VLAN，从允许的 VLAN 列表中去除某些 VLAN
6	Switch(config-if)#end （Ctrl+Z）	返回到特权模式
7	Switch#show interface interface-id Switchport	对配置进行检验。一定要加上 Switchport 关键字，否则会出现 show interface 输出结果
8	Switch#copy running-config startup-config	保存配置

在默认状态下，Trunk 接口允许所有 VLAN 的发送和接口传输。当然，根据需要，我们也可以将拒绝某些 VLAN 通过 Trunk 传输，从而将该 VLAN 限制与其他交换机的通信，或者拒绝某些 VLAN 对敏感数据的访问。需要注意的是，不能从 Trunk 中移除默认的 VLAN1。

Switch(config-if)# switchport trunk allowed vlan {add | all | except | remove} vlan-list 要限制 trunk 传送的 VLAN，从允许的 VLAN 列表中去除某些 VLAN。如执行 Switch2（config-if）#switchport trunk allowed vlan remove 10 之后，VLAN 10 的将不被传递。

配置 Trunk 上允许的 VLAN 列表。使用 add（添加）、all（所有）、except（除外）和 remove（移除）关键字，可以定义允许在 Trunk 上传输的 VLAN。VLAN 列表既可以是一个 VLAN，也可以是一个 VLAN 组。当同时指定若干 VLAN 时，不要在“,”或“-”间使用空格。

7.3.4　利用 Trunk 解决问题

当多台交换机同时被划分为两个或两个以上 VLAN 时，需要创建 Trunk，使不同交换机之间的 VLAN 能够借助于一链路进行通信，否则，VLAN 将被限制在交换机内，无法与其他交换机进行通信。默认状态下，第二层接口自动处于动态的 Switchport 模式，当相邻接口（即借助于双绞线或光纤连接在一起的两个接口）支持 Trunk，并且配置为 Trunk 或动态匹配模式，该链接将作为 Trunk。

1．建立 Trunk 隧道

工程师在排除问题的过程中，对 Switch1 的 fastEthernet 0/2 和 Switch2 的 fastEthernet 0/1 接口分别设置为 Trunk，并在每一个接口都采用 dot1q 协议进行干道封装。

下面是 Switch2 的配置：

```
Switch2(config)# interface fastEthernet 0/1
Switch2(config-if)#Switchport mode trunk                    //设置接口为 Trunk 模式
Switch2(config-if)#Switchport trunk encapsulation dot1q     //设置封装的类型
```

对于 Switch1 上的 fastEthernet 0/2 接口，请和上面的 Switch2 交换机配置相同的封装协议，这样可以避免很多 Trunk 不匹配的问题。

需要注意的是，Trunk 端口默认情况下会传送所有的 VLAN 的通信。要查看 Trunk 接口的信息和允许通过此接口的 VLAN，可以使用命令：show interfas interface-id switchport 输出结果：

```
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 （default）
Trunking Native Mode VLAN: 1 （default）
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Voice VLAN: none （Inactive）
```

```
Appliance trust: none
```

2．测试连通性

工程师在调试完两边的 Trunk 封装之后，在 Switch2 交换机 VLAN2 中有一台主机 Host A 将 IP 地址设置为：192.168.0.1/24，在 Switch1 交换机的 VLAN2 中也有一台主机 Host B 其 IP 地址设置为：192.168.0.2/24，如果在连接 Host A 可以 Ping 通，对 Host B 的话，就可以证明隧道配置没有问题，并已经起到了作用。

但是如果在这两台交换机之中，两个工作站分别在不同的 VLAN 之中，则相互 Ping 对方的话，是不能通信的。

从而说明：不同交换机之间的工作站通过 Trunk 相连接，只有这些工作站在同一个 VLAN 之中才可以相互通信，而不同 VLAN 中的工作站是不能通过 Trunk 来通信的。VLAN 技术将一个大的局域网划分为若干个小的虚拟子网，从而使每一个子网都成为一个单独的广播域，子网之间进行通信必须通过三层设备。当 VLAN 在交换机上划分后，不同 VLAN 间的设备就如同是被物理地分割。也就是说，连接到同一交换机、然而处于不同 VLAN 的设备，就如同被物理地连接到两个位于不同网段的交换机上一样，彼此之间的通信一定要经过路由设备；否则，他们之间将无法得知对方的存在，将无法进行任何通信。