实验 ： VLAN 的配置与管理

一、 实验目的：

1. 了解 Vlan 的相关概念
2. 掌握基于交换机的 Vlan 配置
3. 掌握多台交换机利用 trunk 联通多个 Vlan 的配置

二、 实验环境和准备：

1. 实验环境：联网的计算机网络实验室；
2. 实验时数：2 学时；
3. 实验准备：
   1） 了解 IEEE802.1Q 关于 Vlan 的概念
   2） 了解 IEEE802.1Q 关于 trunk 的概念

三、相关知识点：

什么是 vlan？

VLAN 是英文 Virtual Local Area Network 的缩写，即虚拟局域网。一方面，VLAN 建立在局域网交换机的基础之上；另一方面，VLAN 是局域交换网的灵魂。这是因为通过 VLAN 用户能方便地在网络中移动和快捷地组建宽带网络，而无需改变任何硬件和通信线路。这样，网络管理员就能从逻辑上对用户和网络资源进行分配，而无需考虑物理连接方式。 VLAN 充分体现了现代网络技术的重要特征：高速、灵活、管理简便和扩展容易。是否具有 VLAN 功能是衡量局域网交换机的一项重要指标。网络的虚拟化是未来网络发展的潮流。

VLAN 与普通局域网从原理上讲没有什么不同，但从用户使用和网络管理的角度来看，VLAN 与普通局域网最基本的差异体现在：VLAN 并不局限于某一网络或物理范围，VLAN 中的用户可以位于一个园区的任意位置，甚至位于不同的国家。

VLAN 具有以下优点：

a) 控制网络的广播风暴

采用 VLAN 技术，可将某个交换端口划到某个 VLAN 中，而一个 VLAN 的广播风暴不会影响其它 VLAN 的性能。

b) 确保网络安全

共享式局域网之所以很难保证网络的安全性，是因为只要用户插入一个活动端口，就能访问网络。而 VLAN 能限制个别用户的访问，控制广播组的大小和位置，甚至能锁定某台设备的 MAC 地址，因此 VLAN 能确保网络的安全性。

c) 简化网络管理

网络管理员能借助于 VLAN 技术轻松管理整个网络。例如需要为完成某个项目建立一个工作组网络，其成员可能遍及全国或全世界，此时，网络管理员只需设置几条命令，就能在几分钟内建立该项目的 VLAN 网络，其成员使用 VLAN 网络，就像在本地使用局域网一样。

VLAN 的分类主要有以下几种：

a) 基于端口的 VLAN

基于端口的 VLAN 是划分虚拟局域网最简单也是最有效的方法，这实际上是某些交换端口的集合，网络管理员只需要管理和配置交换端口，而不管交换端口连接什么设备。

b) 基于 MAC 地址的 VLAN

由于只有网卡才分配有 MAC 地址，因此按 MAC 地址来划分 VLAN 实际上是将某些工作站和服务器划属于某个 VLAN。事实上，该 VLAN 是一些 MAC 地址的集合。当设备移动时，VLAN 能够自动识别。但当网络规模很大，设备很多时，会给管理带来难度并且影响设备效率。

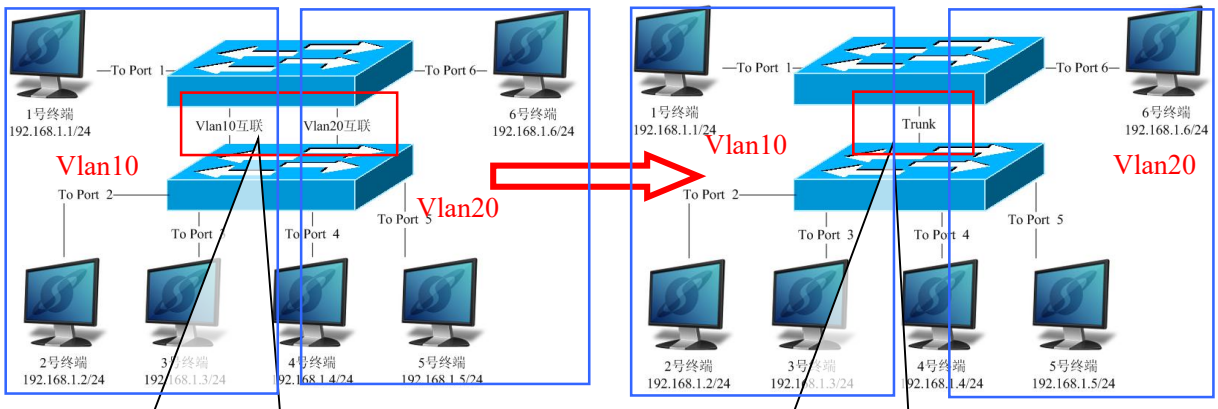
c) 基于第 3 层的 VLAN

基于第 3 层的 VLAN 是采用在路由器中常用的方法：IP 子网和 IPX 网络号等。其中，局域网交换机允许一个子网扩展到多个局域网交换端口，甚至允许一个端口对应于多个子网。

本次实验着重讲解的是基于端口的 VLAN 配置方法。

什么是 trunk?

在路由与交换领域，VLAN 的端口聚合叫 TRUNK 或 TRUNKING（前面我们学习的交换机端口聚合英文名称也叫 trunk 但是用途完全不同）。所谓的 TRUNKING 是用来在不同的交换机之间进行连接，以保证在跨越多个交换机上建立的同一个 VLAN 的成员能够相互通讯。其中交换机之间互联用的端口就称为 TRUNK 端口。与一般的交换机的级联不同，TRUNKING 是基于 OSI 第二层的。假设没有 TRUNKING 技术，如果你在 2 个交换机上分别划分了多个 VLAN（VLAN 也是基于 Layer2 的），那么分别在两个交换机上的 VLAN10 和 VLAN20 的各自的成员如果要互通，就需要在 A 交换机上设为 VLAN10 的端口中取一个和交换机 B 上设为 VLAN10 的某个端口作级联连接。VLAN20 也是这样。那么如果交换机上划了 10 个 VLAN 就需要分别连 10 条线作级联，端口效率就太低了。 当交换机支持 TRUNKING 的时候，事情就简单了，只需要 2 个交换机之间有一条级联线，并将对应的端口设置为 Trunk，这条线路就可以承载交换机上所有 VLAN 的信息。这样的话，就算交换机上设了上百个个 VLAN 也只用 1 个端口就解决了。



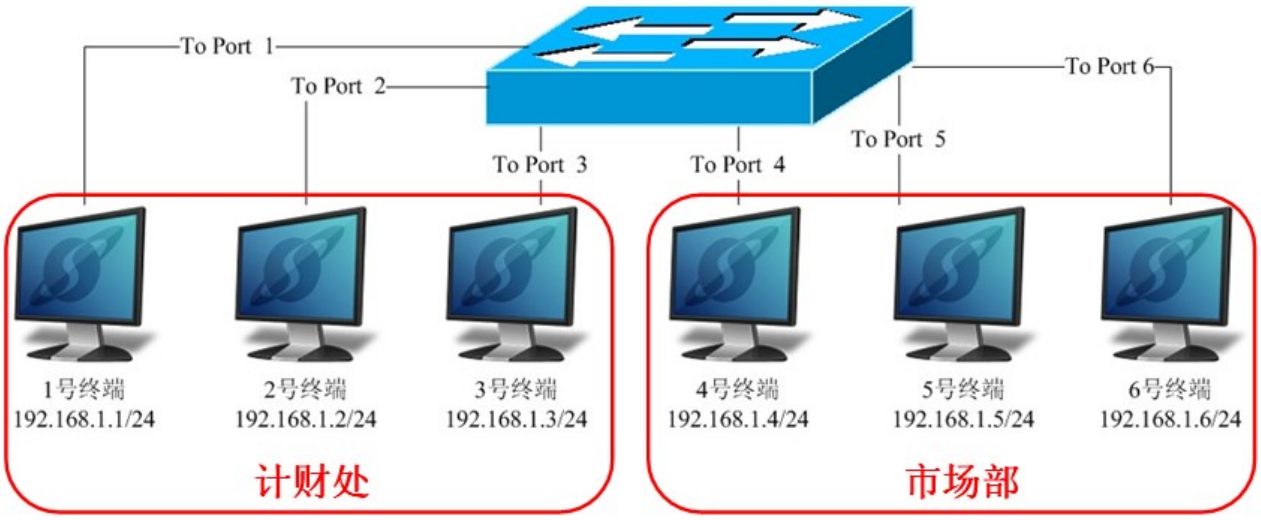
如果有多个 vlan 跨交换机互联就要用多条级联线，浪费了大量交换机的端口。

采用了 trunk 技术之后，大大节省了交换机的级联端口占用。

四、**实验内容：**

公司计财处和市场部分别有三台 PC 终端两部门合用一台交换机 DCS3950-26c，公司基于安全的考虑，希望在不增加投入的情况下将两个部门在逻辑上进行分割，相互不能进行互访。

【解决方案】通过使用 Vlan 的安全特性，将一台交换机在逻辑上划分成两台相互不关联的交换机，从而使两个部门不能相互访问。



实验步骤：

（1） 根据上面的拓扑图搭建网络实体环境，对每台 PC 终端进行 IP 地址的配置

（2） 在各台终端之间使用 ping 命令测试其相互间的连通性,验证示例如下

```
pc>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=111ms TTL=128
Reply from 192.168.1.4: bytes=32 time=62ms TTL=128
Reply from 192.168.1.4: bytes=32 time=47ms TTL=128
Reply from 192.168.1.4: bytes=32 time=63ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 47ms, Maximum = 111ms, Average = 70ms
```

（3） 对交换机 3950-24 进行基于端口的 VLAN 设置

a) 创建 **vlan10**(代表计财处)和 **vlan20**（代表市场部）

```
Switch>
Switch>en
Switch#config t
Enter configuration commands, one per line.   End with CNTL/Z.
Switch(config)#vlan 10                        //创建 vlan 10
Switch(config-vlan)#exit
Switch(config)#vlan 20                        //创建 vlan20
Switch(config-vlan)#exit
```

b) 检测创建的 vlan 是否生效

```
Switch#show vlan
VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   VLAN0010                            active    \\vlan10 创建成功
20   VLAN0020                            active    \\vlan20 创建成功
1002 fddi-default                        act/unsup
1003 token-ring-default                  act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1
Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------



Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

如图，我们已经创建了两个 vlan，但 2 个 vlan 都没有进行端口绑定，所有的端口都归属与交换机的默认 vlan1 中

c) 将 PC 终端对应的交换机端口绑定到各自的 vlan 中，对于这个案例来说，我们将交换机的 1、2、3 端口绑定到 vlan10 中，4、5、6 端口绑定到 vlan20 中

```
switch#
switch#config t                                  \\进入全局模式
switch(config)#int f0/1                          \\进入第一个以太网口
Switch(config-if)#switchport access vlan 10      \\将该端口绑定至 vlan10
```

```
Switch(config-if)#exit                                    \\退出端口配置模式
switch(Config)#
```

同样的方法将 2、3、4、5、6 号终端绑定到不同的 vlan 中去。

d) 绑定完成之后,我们再次使用 show vlan 命令来确定我们的交换机物理端口是否和 vlan 绑定成功

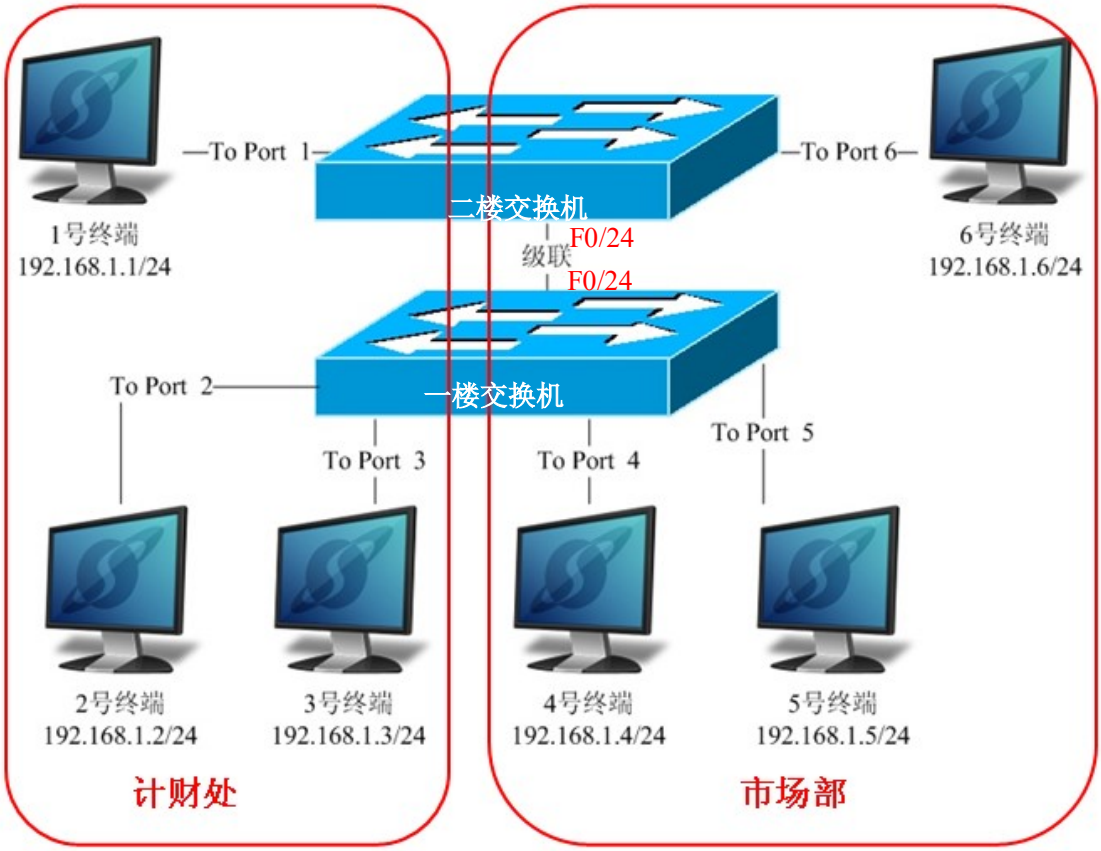
```
switch(Config)# exit
switch#show vlan
VLAN Name                                        Status    Ports
---- ------------------------------- --------- -------------------------------
1    default                                     active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                           Fa0/23, Fa0/24
10   VLAN0010                                    active    Fa0/1, Fa0/2, Fa0/3
20   VLAN0020                                    active    Fa0/4, Fa0/5, Fa0/6
1002 fddi-default                                act/unsup
1003 token-ring-default                          act/unsup
1004 fddinet-default                             act/unsup
1005 trnet-default                               act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1
Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
 --More--
```

从上面的命令我们可以看出，vlan10 和 vlan20 都分别绑定了相应的端口，此时交换机在逻辑上已经分为了两台无相不关联的交换机，对应不同 vlan 的交换机物理端口是相互之间不能互通的。

（4） 检测实验配置结果，在部门用 ping 命令测试各台 PC 终端是否互联互通；跨部门用 ping 命令测试各台 PC 终端是否能互联互通，并将结果记录下来。

五、进阶练习：跨交换机的 vlan 划分

如下拓扑，公司的计财处和市场部现在由两个楼层交换机将两个部门互联，两个交换机用各自的 24 号端口进行级联，为了不增加布线成本，利用现有的两台交换机将两个部门在逻辑上进行分割，使得两个部门不能互相访问。



【解决方案】我们已经知道 vlan 可以在逻辑上将一台交换机划分成多台交换机用，但在上面的网络环境中，需要将两台交换机在逻辑上分割成四台交换机，这样就需要两条级联线和占用四个交换机端口用于级联，而实际环境中不允许我们用两条级联线来连接交换机。基于以上条件，我们可以使用 trunk 技术来解决这一问题。

实验步骤：

（1）如图搭建网络实体环境。将一楼交换机的 2、3 号端口划分到 vlan10 ，一楼的 4、5 号端口划分到 vlan20，二楼交换机的 1 号端口划分到 vlan10，二楼交换机的 6 号端口划分到 vlan20.完成了这步工作之后，楼层内部门内的 PC 终端可以相互通讯，但是跨楼层的 pc 终端并不能互联。

（2）使用 trunk 技术将两台交换机的 vlan 信息共享。这就需要我们在两台交换机的级联端口即本案例的交换机 24 号物理端口进行 trunk 设置

```
Switch(config)#int f0/24                          //进入交换机的第 24 号物理端口
Switch(config-if)#switchport mode trunk           //将端口设置为 trunk 模式
Switch(config-if)# switchport trunk allowed vlan all   //允许所有的 vlan 信息通过该 trunk
```

（3）用 show vlan、show run 等 命令来查看 vlan 和 trunk 的信息，并记录。

（4）使用 ping 命令来测试跨交换机相同部门和不同部门的终端连通性

六、**思考题：**

（1）简述什么是 IEEE802.1Q 的数据封装及其作用。

（2）使用什么方式可以控制 trunk 允许通过某些 vlan 通过，试举例说明。