计算机网络实验实验报告

学院（系）名称：信息学院

姓名	高星杰	**学号**	2021307220712	**专业**	计算机科学与技术
班级	21 级 2 班	**实验项目**	LAN 的组建互连及 VLAN 划分通信		
课程名称		计算机网络实验		**课程代码**	3103009336
实验时间		2023 年 11 月 23 日星期四		**实验地点**	逸夫楼 C207

考核内容	目的和原理 40	内容及过程分析 30	实验方案设计 10	实验结果（结论正确性以及分析合理性）20	**成绩**	
各项得分						
考核标准	○原理明确 ○原理较明确 ○原理不明确	○分析清晰 ○分析较清晰 ○分析不清晰	○设计可行 ○设计基本可行 ○设计不可行	○结论正确，分析合理 ○结论正确，分析不充分 ○结论不正确，分析不合理	**教师签字：**	

1. 实验目的

1.1 掌握 LAN 的组建
1.2 掌握 LAN 的互连
1.3 理解 LAN 的设计思想
1.4 掌握 VRP 的使用及 Switch 原理
1.5 掌握 VLAN 划分方法和 VLAN 间通信

2. 实验原理

在开始实验之前我们要先了解一些原理，我们才能基于原理开始分析、设计，并且对原理的认识和理解决定着我们后面实验步骤的质量和是否能流畅的解决问题，所以本次实验报告实验原理和实验过程所占比例较大。

这里我们通过几个自问自答的问题来逐层递进的来理解本次实验的实验原理。**面向问题来理解理论，这样的理解将会更加深入，记忆也更加深刻。**

(1)什么是局域网（Local Area Network）？

LAN 表示 Local Area Network，本地局域网。一个 LAN 表示一个广播域，含义是：LAN 中的所有成员都会收到任意一个成员发出的广播包。而两个 LAN 中的成员是无法直接进行广播的，但是可以间接广播。LAN 是一个覆盖地理范围相对较小的高速容错数据网络,它包括工作站、个人计算机、打印机和其它设备。提供包括对设备和应用的共享访问、互联用户的文件交换、电子邮件和其它应用程序间的通信等。同时局域网中的 LAN 协议在 OSI 参考模型的物理层和数据链路层之间发挥作用

局域网的典型特性如下：高数据率　短距离　低误码率

(2) 什么是 VLAN(Virtual Local Area Network)?

VLAN(Virtual LAN)，翻译成中文是“虚拟局域网”。LAN 可以是由少数几台家用计算机构成的网络，也可以是数以百计的计算机构成的企业网络。VLAN 所指的 LAN 特指使用路由器分割的网络——也就是广播域。虚拟局域网（VLAN）是在局域网（LAN）的逻辑上划分成多个广播域，每一个广播域就是一个 VLAN。

(3) VLAN 和 LAN 的区别是什么?

它们之间的主要区别在于：

范围：

LAN 是物理上连接在一起的设备组成的网络，通常在一个物理位置或建筑内。

VLAN 是在一个或多个 LAN 上创建的逻辑上隔离的网络，可以跨越不同的物理位置或交换机。

隔离和安全：

LAN 中的设备彼此直接连接，通常位于同一物理网络中，因此可能存在安全风险。

VLAN 通过在交换机上配置逻辑划分，将不同的设备划分为虚拟上的不同网络，提高了安全性和隔离性。

管理和灵活性：

LAN 的管理相对固定，需要物理重新布线才能更改网络结构。VLAN 可以通过软件配置和管理，更加灵活地组织和重新配置网络，无需物理改变布线。

成本和效率：

LAN 的建设可能需要更多的物理设备和布线，而 VLAN 可以利用现有的网络基础设施实现逻辑分割，节约成本和提高效率。

总的来说，LAN 是指物理上连接的局域网，而 VLAN 则是在物理网络基础上建立的逻辑隔离的虚拟网络，能够更灵活、安全地管理网络资源。

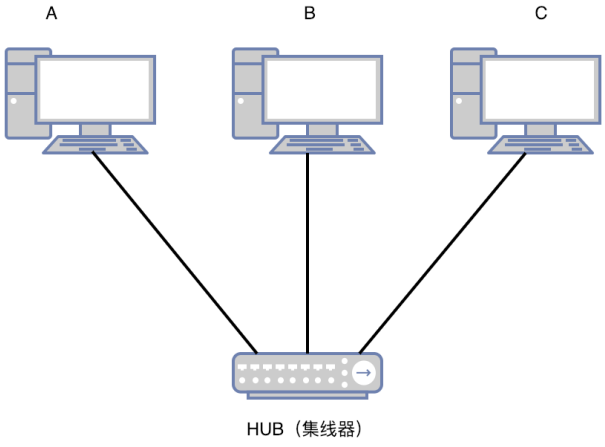
(4) 为什么要使用 VLAN？VLAN 是为了解决什么问题的？

在清楚了 VLAN 和 LAN 的区别之后，我们很容易就会想到这个问题。任何设计都不是无缘由的，都是有迹可循的，都是有他的理由的，所以想要深入的了解他们就要了解他们的“背后的故事”。

在此让我们先复习一下广播域的概念。广播域，指的是广播帧(目标 MAC 地址全部为 1)所能传递到的范围，亦即能够直接通信的范围。严格地说，并不仅仅是广播帧，多播帧(Multicast Frame)和目标不明的单播帧(Unknown Unicast Frame)也能在同一个广播域中畅行无阻。

本来，二层交换机只能构建单一的广播域，不过使用 VLAN 功能后，它能够将网络分割成多个广播域。

那么，为什么需要分割广播域呢?那是因为，如果仅有一个广播域，有可能会影响到网络整体的传输性能。具体原因请往下看。



上图为最基本的 LAN 布局。如果设备间想要通讯，必须要获取到对方的 MAC 地址。

举例：A 发信息给 C，A 并不知道 C 的 MAC 地址。此时通过 ARP 协议（Address Resolution Protocol；地址解析协议；）获取 C 的 MAC 地址，A 先要广播一个包含目标 IP 地址的 ARP 请求到链接在集线器上的所有设备上，C 接受到广播后返回 MAC 地址给 A，其他设备则丢弃信息。至此已经建立设备间通信的准备条件。

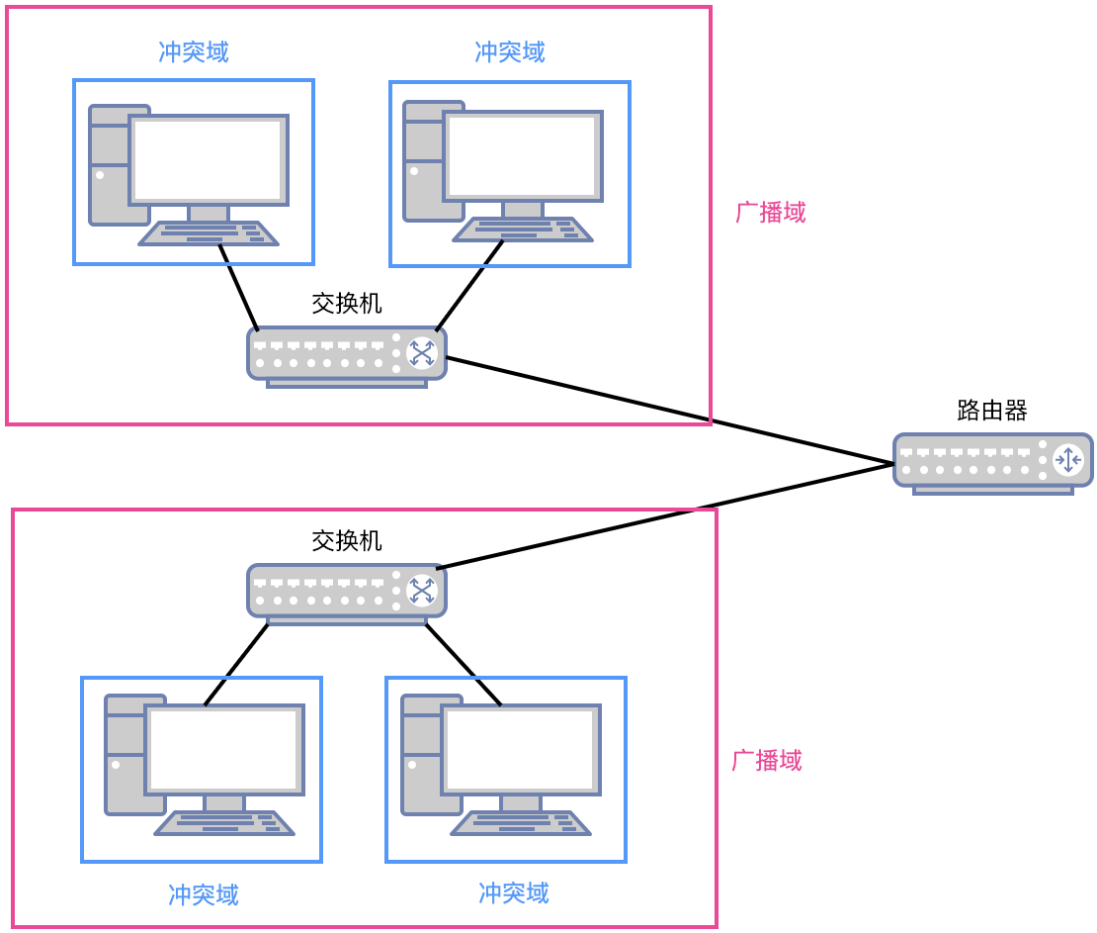
链接在集线器中的设备都在同一个冲突域和广播域中。此时的冲突域就是广播域。简单理解就是在这种布局中，一次只能一台设备发送信号且其他设备都能接受该信号。

但是需要注意的是，这个 ARP 请求原本是为了获得计算机 C 的 MAC 地址而发出的。也就是说：只要计算机 C 能收到就万事大吉了。可是事实上，数据帧却传遍整个网络，导致所有的计算机都收到了它。如此一来，**一方面广播信息消耗了网络整体的带宽，另一方面，收到广播信息的计算机还要消耗一部分 CPU 时间来对它进行处理。造成了网络带宽和 CPU 运算能力的大量无谓消耗。当设备越来越多的时候每个设备都发送一个广播，交换机需要把每个广播复制下发到所有设备，这个开销就很可怕了。**

读到这里，您也许会问：广播信息真是那么频繁出现的吗?

答案是：是的!实际上广播帧会非常频繁地出现。利用 TCP/IP 协议栈通信时，除了前面出现的 ARP 外，还有可能需要发出 DHCP、RIP 等很多其他类型的广播信息。如果整个网络只有一个广播域，**那么一旦发出广播信息，就会传遍整个网络，并且对网络中的主机带来额外的负担**。因此，在设计 LAN 时，需要注意如何才能有效地分割广播域。

所以我们使用路由器对广播域进行隔离如下图所示：



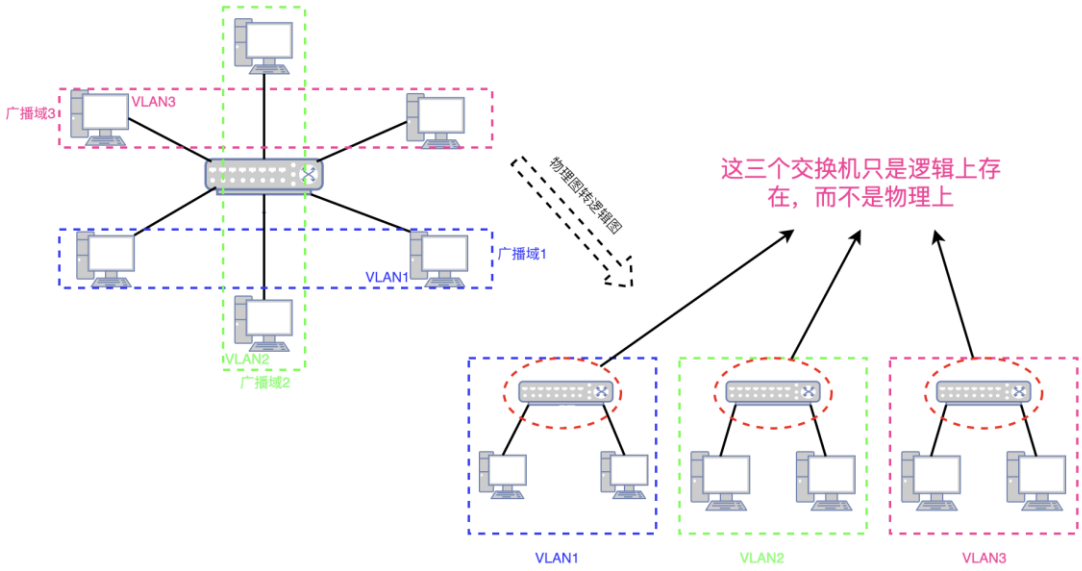
广播域的隔离：

当路由器收到广播时，会把它自动丢弃，不会转发到路由器的其他端口，实现了广播域的分割。这也是路由器存在的意义，如果将全网都集中在一个广播域中则容易引发广播，进而导致全网瘫痪。

VLAN 是如何解决问题的：

虚拟局域网（VLAN）是在局域网（LAN）的逻辑上划分成多个广播域，每一个广播域就是一个 VLAN。下图为交换机划分虚拟局域网。交换机把一个广播域划分成了 3 个广播域，物理上这些设备在一个交换机上，但是逻辑上已经分别划分到三个交换机上，所以会有三个局域网（虚拟局域网），三个广播域。

如下图所示



我们既然已经基本了解了 VLAN，我们肯定又会产生另一个问题 VLAN 是如何实现的呢？

(5) VLAN 实现原理是什么？

1. 静态 VLAN

静态 VLAN 又被称为基于端口的 VLAN（PortBased VLAN）。是为了明确指定哪个 Port 属于哪个 VLAN ID。

在 VLAN 管理员最初配置交换机 Port 和 VLAN ID 的对应关系时，就已经固定了这种对应关系，即一个 Port 只能对应一个 VLAN ID，之后无法进行更改，除非管理员再重新配置。

当一台设备接到这个 Port 上的时候，怎么判断该主机的 VLAN ID 与 Port 对应呢，这里是根据 IP 配置决定的，我们知道每个 VLAN 都有一个子网号，并对应着哪些 Port，如果设备要求的 IP 地址和该 Port 对应的 VLAN 的子网号不匹配，则连接失败，该设备将无法正常通信。所以除了连接到正确的 Port 外，也必须给设备分配属于该 VLAN 网络段的 IP 地址，这样才能加入到该 VLAN 中。

由于需要一个个端口地指定，因此当网络中的计算机数目超过一定数字（比如数百台）后，设定操作就会变得烦杂无比。并且，客户机每次变更所连端口，都必须同时更改该端口所属 VLAN 的设定——这显然不适合那些需要频繁改变拓补结构的网络。

2. 动态 VLAN

动态 VLAN 则是根据每个端口所连的计算机，随时改变端口所属的 VLAN。这就可以避免上述的更改设定之类的操作。动态 VLAN 可以大致分为 3 类：

（1）基于 MAC 的 VLAN

基于 MAC 地址的 VLAN ，就是通过查询并记录端口所连的计算机网卡的 MAC 地址来决定端口的所属。假定有一个 MAC 地址 “A” 被交换机设定为属于 VLAN 10，那么不论 MAC 地址为 “A” 的这台计算机连在交换机哪个端口，该端口都会被划分到 VLAN 10 中去。计算机连在端口 1 时，端口 1 属于 VLAN 10 ；而计算机连在端口 2 时，则是端口 2 属于 VLAN 10。

基于 MAC 地址的 VLAN ，在设定时必须调查所连接的所有计算机的 MAC 地址并加以登录。而且如果计算机交换了网卡，还是需要更改设定。

（2）基于 IP 的 VLAN

基于子网的 VLAN，则是通过所连计算机的 IP 地址，来决定端口所属 VLAN 的。不像基于 MAC 地址的 VLAN，即使计算机因为交换了网卡或是其他原因导致 MAC 地址改变，只要它的 IP 地址不变，就仍可以加入原先设定的 VLAN。

因此，与基于 MAC 地址的 VLAN 相比，能够更为简便地改变网络结构。IP 地址是 OSI 参照模型中第三层的信息，所以我们可以理解为基于子网的 VLAN 是一种在 OSI 的第三层设定访问链接的方法。

（3）基于用户的 VLAN

基于用户的 VLAN，则是根据交换机各端口所连的计算机上当前登录的用户，来决定该端口属于哪个 VLAN。这里的用户识别信息，一般是计算机操作系统登录的用户，比如可以是 Windows 域中使用的用户名。这些用户名信息，属于 OSI 第四层以上的信息。

而本次实验由于用不到组建很复杂的网络，所以使用的是静态 VLAN，并且我们也能通过组件静态的 VLAN 我们也可以感受其设计思想。

除此之外我们要想实现 VLAN，我们就要借助支持 VLAN 的交换机，比如实验室提供的华为交换机，该如何使用它呢？请继续往下看。

（6）我们该如何操控交换机来实现虚拟局域网？

和操作计算机一样我们不可能直接对硬件进行操控，我们要通过操作系统来操作，操作交换机也不例外，我们通过操控交换机的操作系统 VRP（Versatile Routing Platform）来，实现我们对交换机的一些列设置。

什么是 VRP ？ VRP 是华为公司从低端到高端的全系列路由器、交换机等数据通信产品的通用网络操作系统，就如同微软公司的 Windows 操作系统之于 PC,苹果公司的 iOS 操作系统之于 iPhone。VRP 可以运行在多种硬件平台之上，并拥有一致的网络界面、用户界面和管理界面，可为用户提供灵活而丰富的应用解决方案。VRP 就是华为设备的操作系统。

如何操作 VRP? 我们使用 Xshell 远程连接软件来连接到 VRP 的控制终端，我们可以在计算机上输入各种命令来操作 VRP，来让交换机实现我们所想要的功能。

回答了上面的几个问题，我们基本上已经讲清楚了本次实验所用的实验原理。接下来我们就可以进行实验分析。

3. 实验分析：

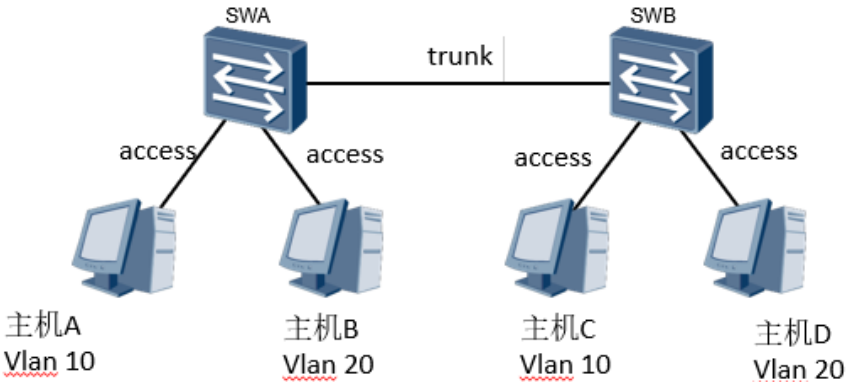
根据需求，我们是要搭建两个物理上连通但是逻辑上不连通的局域网，对于此我们就实习两件事：

1. 局域网的搭建
2. 虚拟局域网的划分

局域网的搭建与互连：使用一个或多个交换机设备，与主机组成局域网链路。在不连接互联网的情况下，局域网间的主机设备可以通过交换机设备完成数据交换的工作。交换机负责转发、传输数据。

虚拟局域网的划分：搭建完局域网后我们可以发现的一个局域网的主机是可以互相传送数据的，我们要对广播域进行划分，为了验证虚拟局域网是成功划分，**我们就要设计一个原本能够互联互通的网路，但是在局域网划分后就不能互相传送数据的网络。**

所以我们可以根据以上分析设计出如下概念图：



主机 A 和主机 C 位于一个 VLAN 中，主机 B 和主机 D 位于一个 VLAN 中。

在交换机的初始状态下，所有物理端口属于同一个 VLAN 1，即无划分状态，主机 A 和主机 B 是可以自由的互通的，同时主机 A 也能和其他的主机 CD 进行互通的，其他主机跟主机 A 是相同的。

然后通过创建不同的 VLAN，并将物理端口分配到其他 VLAN 中，实现相同 VLAN 内的主机可以互连，不同 VLAN 的主机不可以互连。虽然主机可能处于同一个 LAN 中，但其若所属 VLAN 不同，则不能互通。

4. 实验设计：

在经过上面的实验分析，我们可以大致的设计出实验的基本的内容。

1. 局域网的搭建

首先将局域网与小组内的 4 台主机和 2 台交换机，用线连接在一起。具体如何连接在实验过程中涉及。

其次将 4 台主机的 IP 地址进行配置，以便后续进行通讯。

然后验证局域网的搭建是否有效，及具体步骤可以通过 ping 和抓包来验证，基本思想就是进行主机与主机间的互联通信，检查是否成功。

2. 虚拟局域网的划分

首先使用 Xshell 连接交换机的 VRP 终端，配置一些初始设置，并学习一些基本的命令，准备配置虚拟局域网。

然后使用命令对每个端口进行配置，划分为不同的 VLAN，并且将 Trunk 端口配置，连接两个交换机。

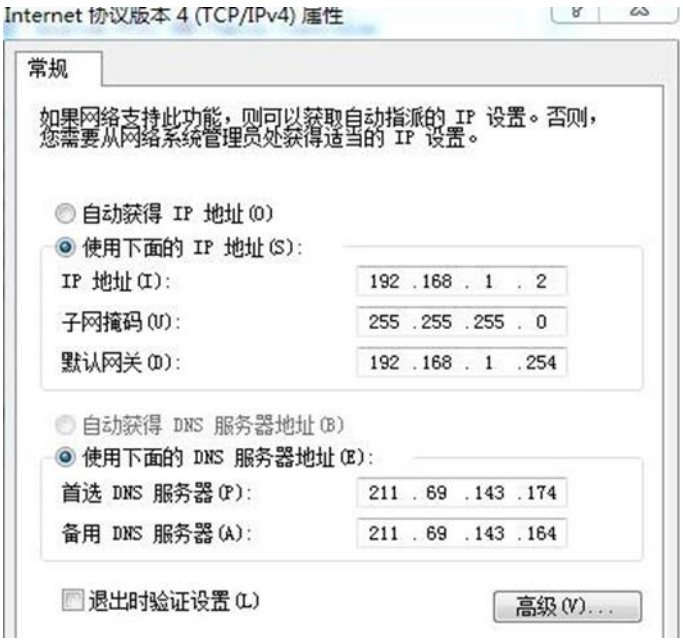
最后测试 VLAN 间的通讯和测试不同的 VLAN 间的通讯

5. 实验过程：

(1)组建局域网

首先使用交换机进行组内互连。交换机接电源后，使用网线将组内的 PC 主机连接到交换机的端口上。

确认连接成功后，修改 PC 主机的本地网络设置，将 IPv4 地址设置为 192.168.1.x。默认网关设置为
192.168.1.254。



（2）使用 ping 指令进行组内互联测试，测试结果显示连接成功

实验课上将所有组的交换机的连接成环后，测试连接其他组的主机

经过上面测试我们发现局域网已经组建成功了，然后接下来就是使用 VRP 进行虚拟局域网的划分。

（3）使用 VRP 进行初始化配置

使用 Xshell 进入 VRP，并且登录账号后，进入系统视图

```
  Press any key to get started


Login authentication


Username:admin
Password:
Error: Authentication failed.

  Error:Logged Fail!

  Please retry after 5 seconds.

Username:admin
Password:
<Huawei>sys
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
```

使用 display clock 查看系统时钟

```
[Huawei]display clock
2023-11-29 02:09:53
Wednesday
Time Zone(Default Zone Name) : UTC+00:00
```

使用 header 指令修改登录和退出的信息

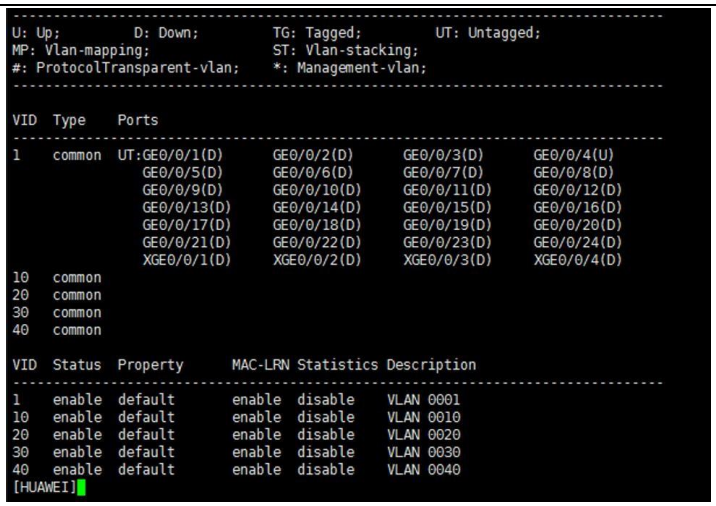
```
[Huawei]header login i
[Huawei]header login information "WelCome!"
[Huawei]h
[Huawei]header shell i
[Huawei]header shell information "Bye!"
```

查看当前配置

```
[Huawei-GigabitEthernet0/0/0]display  current-configuration
[V200R007C00SPCb00]
#
 header shell information "Bye!"
 header login information "WelCome!"
#
 drop illegal-mac alarm
#
vlan batch 10
#
pki realm default
 enrollment self-signed
#
ssl policy default_policy type server
 pki-realm default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 local-aaa-user password policy administrator
  password history record number 0
  undo password alert original
 domain default
 domain default_admin
```

(4) 使用 VRP 进行虚拟局域网划分

1) 使用 vlan batch 指令，创建 VLAN10 VLAN20 VLAN30 VLAN40



如图所示可以看到已经有 5 个 VLAN 了，我们创建了 4 个，自动初始化了 1 个，在初始状态下所有物理端口都被分配给了自动初始化的那个，所以一开始我们就是可以实现互联。

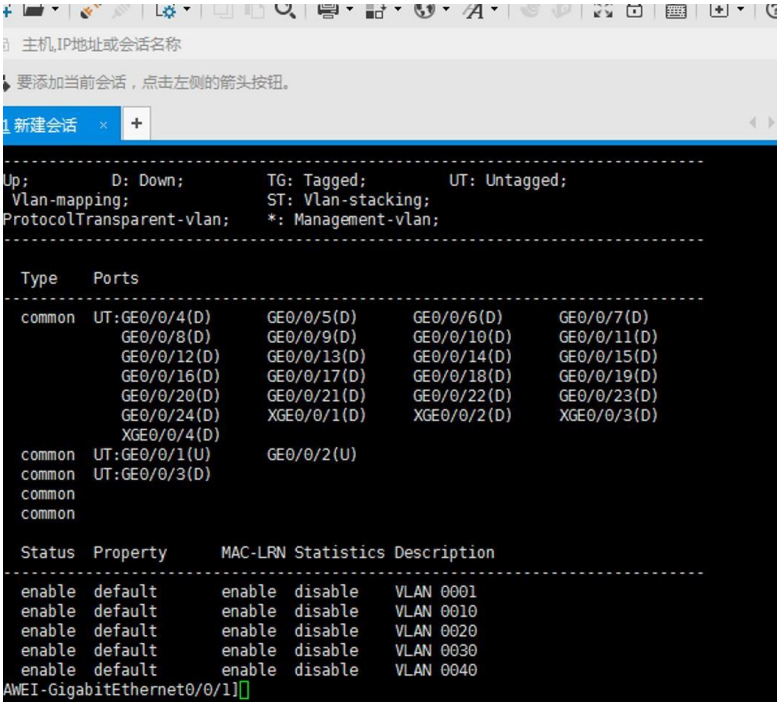
2) 使用 interface GigabitEthernet0/0/1，管理 001 号端口；

使用 port link-type access，设置端口类型为 access（access 端口只能属于一个 VLAN）。

使用 port default vlan 10，将该端口分配到 vlan 10 中。

使用 interface GigabitEthernet0/0/2，重复上述操作，将该端口也分配到 vlan 10 中。

使用 interface GigabitEthernet0/0/3，重复上述操作，将该端口分配到 vlan 20 中。



3) 两台交换机配置 Trunk 连接

使用 interface GigabitEthernet0/0/1，管理 001 号端口；

使用 port link-type trunk，设置端口类型为 trunk（中继接口，可以属于多个 vlan）。

使用 port trunk allow-pass vlan 10 to 20，使得该中继端口可以访问 vlan10 和 vlan20。

```
[HUAWEI-GigabitEthernet0/0/2]
Apr  2 2000 01:00:16+08:00 HUAWEI DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.19
3.1 configurations have been changed. The current change number is 5, the change loop
unt is 0, and the maximum number of records is 4095.
[HUAWEI-GigabitEthernet0/0/2]quit
[HUAWEI]interface GigabitEthernet 0/0/3
[HUAWEI-GigabitEthernet0/0/3]port default vlan 20
[HUAWEI-GigabitEthernet0/0/3]dis vlan
The total number of VLANs is: 5
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
1    common  UT:GE0/0/1(D)      GE0/0/4(U)      GE0/0/5(D)      GE0/0/6(D)
                GE0/0/7(D)      GE0/0/8(D)      GE0/0/9(D)      GE0/0/10(D)
                GE0/0/11(D)     GE0/0/12(D)     GE0/0/13(D)     GE0/0/14(D)
                GE0/0/15(D)     GE0/0/16(D)     GE0/0/17(D)     GE0/0/18(D)
                GE0/0/19(D)     GE0/0/20(D)     GE0/0/21(D)     GE0/0/22(D)
                GE0/0/23(D)     GE0/0/24(D)     XGE0/0/1(D)     XGE0/0/2(D)
                XGE0/0/3(D)     XGE0/0/4(D)
10   common  UT:GE0/0/2(D)
             TG:GE0/0/1(D)
20   common  UT:GE0/0/3(D)
             TG:GE0/0/1(D)
```

（5）测试 VLAN 内和 VLAN 外通信

首先将测试主机网线接入端口 003 与 001，进行 ping 测试

```
:\Users\lenovo>ping 192.168.1.3

正在 Ping 192.168.1.3 具有 32 字节的数据:
请求超时。
请求超时。
来自 192.168.1.2 的回复: 无法访问目标主机。
来自 192.168.1.2 的回复: 无法访问目标主机。

92.168.1.3 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 2, 丢失 = 2 (50% 丢失),
```

由结果所示不在一个虚拟局域网内无法通信。

而同一个虚拟局域网中的可以访问，如下图

```
C:\Users\lenovo>ping 192.168.1.4

正在 Ping 192.168.1.4 具有 32 字节的数据:
来自 192.168.1.4 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.4 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.4 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.4 的回复: 字节=32 时间<1ms TTL=64

192.168.1.4 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):
```

6. 结论与分析：

(1) 遇到的问题及解决方案

问题一：配置虚拟局域网时所有操作做完后仍然不能连通

解决方案：查看接口的状态表，发现由一个 D 而不是 U，也就是此接口没有在工作，然后检查发现是接口松了，没有插紧。

反思：养成了查看的端口的状态表，判断端口是否工作的习惯，知道了如何正常工作的基本流程，如果出错了就知道可能在那个流程上出错了。

问题二：帮同学解决问题时发现有 vlan 下一个端口也没有在工作

解决方案：首先查看接口的状态发现虽然 vlan 下没有一个端口在工作，但是所有端口中还是有 5 个端口在工作，所以判断是设置的端口时配置错端口了，配置了没有连接的端口，所以肯定还是不工作，只要改变连接端口，或者是改变端口配置，两者选其一就行的。

反思：要首先理解的基本的原理，不然只跟着 ppt 上的命令做，很容易生搬硬套，然后出现问题也没有办法去改。

(2) 实验心得与感悟

本次实验更让我感受到计算机专业真的是少数讲课和实际相差不远的专业，不像其他专业一样学的几乎不能实际应用，我们学到的理论立马就可以在实践中检验，是看得到摸得着的。让我更加确信这就是我所喜欢的专业。

其次我更加深刻的认识到了两点，一是理解原理的重要性，如果我们没有理解原理，那么它相对于我们就是一个的黑盒，出问题后也没有办法解决，所以我们也要学原理，再做应用，不然我们会花更多的时间的，学习原理反而让我们节省时间。二是要用面向问题的思维去学习，理论的提出都是和问题相关的，我们想要搞清楚理论的来龙去脉就要搞清楚它的提出是为了解决什么问题，它用途的是什么。这样学习会事倍功半。

(针对实验结果，对其正确性、创新性进行分析；写出遇到的问题及其解决方案，本次实验心得体会）

【过程记录（源程序、测试用例、测试结果等）】