实验五 虚拟局域网的划分

一、实验目的

通过本次实验，使学生深入理解虚拟局域网的工作原理，学生将会对交换机的配置方法有一个初步的了解，并熟悉使用交换机的虚拟局域网配置的常用命令，并且能对虚拟局域网配置是否正确进行检测。

二、实验原理

如今，局域网变得越来越拥塞，而交换技术正是解决这一问题的方法之一。它可以减少网络的流量，并增加网络带宽。目前在数据通信中，大多数交换设备都只执行两类基本操作：转发数据帧和维护交换操作（构造并维护交换表）。

连接局域网网段的交换机都有一个可寻址存储器（CAM，Content-addressable memory）用来存储MAC地址表（交换表），该表记录了发往目的地址的数据帧需要转发的端口号。

交换机采用自学习算法自主进行记录设备的接口连接信息，并且采用STP生成树协议解决数据帧可能会产生的兜圈子问题。交换机（第二层交换机，即数据链路层）通过收到的数据帧（也称MAC帧）的目的地址来决定该帧需要从哪个端口转发。它看不到数据帧中的数据部分（网络层数据）。如果交换机不知道帧应该发送到哪里（交换表里没有该项），就向除接收端口之外的其他所有的端口广播该帧。当某个端口收到一个帧，而交换表里没有该帧的源地址时，交换机就把该地址和相应的端口存到交换表里。

在交换机每次存储地址时，地址都被打上时间标记。这使得该地址能在交换机里存储一段时间。如果在这段时间内某个地址被引用，则该时间将会被重新设定（说明是此地址和相应端口没有发生改变）。如果在设定的时间内该地址没有被引用，则交换机就会向该端口发送一个发现帧来询问通向该端口的主机的硬件地址是否发生改变。

交换机使用两种方式来转发数据帧：

1）存储转发：当交换机把整个数据帧接收下来之后才进行转发工作。

2）直通交换：由于数据帧的目的地址字段在最前面，所以，当交换机收到数据帧的目的地址字段之后就马上进行转发工作。

两种交换方式各有优缺点：第1种转发方式的时延大，但能过滤出接收到的错误帧；第2种转发方式虽能减少数据帧的转发时延，但当交换机检验到数据帧有错误时已经发送出去大部分了。

1996年，Cisco公司最早提出了虚拟局域网VLAN（Virtual Local Area Network）技术。它是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段从而实现虚拟工作组的技术。但有关VLAN的标准IEEE 802.1Q在1999年6月由IEEE委员会颁布实施。随着几年来的发展，VLAN技术得到广泛的支持，在大大小小的企业网络中被广泛应用，成为当前最为热门的一种以太局域网技术。本次实验就要介绍交换机的一个最常见技术应用——VLAN技术。

1. **什么是VLAN？**

在共享网络中，一个物理的网段就是一个广播域（局域网，LAN）。而VLAN技术的出现，使得管理员根据实际应用需求，把同一物理局域网内的不同用户逻辑地划分成不同的广播域（虚拟局域网，VLAN），每一个VLAN都包含一组有着相同需求的计算机工作站，与物理上形成的LAN有着相同的属性。由于它是从逻辑上划分，而不是从物理上划分，所以同一个VLAN内的各个工作站没有限制在同一个物理范围中，即这些工作站可以在不同物理LAN网段。

由VLAN的这些特点可知：VLAN是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段从而实现虚拟工作组的技术。这一技术主要应用于交换机和路由器中，其主流应用还是在交换机之中。但又不是所有交换机都具有此功能，只有VLAN协议的第三层以上交换机才具有此功能，这一点可以查看相应交换机的说明书即可得知。

注意：VLAN不是VPN（虚拟专用网）。

在同一个VLAN中的工作站，不论它们实际与哪个交换机连接，它们之间的通信就好像在独立的交换机上一样。同一个VLAN中的广播只有VLAN中的成员才能听到，而不会传输到其他的VLAN中去。这样可以很好的控制不必要的广播风暴的产生，从而有助于提高网络的安全性，控制网络流量，形成虚拟工作组，动态管理网络。

VLAN是为解决以太网的广播问题和安全性而提出的一种协议，它在以太网帧的基础上增加了VLAN头，用VLAN ID把用户划分为更小的工作组，限制不同工作组间的用户互访，每个工作组就是一个虚拟局域网（如图1）。

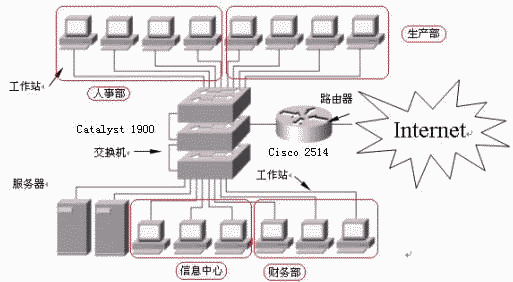


图1 虚拟局域网示例

所连的用户主要分布于四个部分，即：生产部、财务部、信息中心和人事部。本例主要对这四个部分用户单独划分VLAN，从而在逻辑上将以上4个部门分配至不同的局域网中，从而确保相应部门网络资源不被盗用或破坏。

现为了公司相应部分网络资源的安全性需要，特别是对于像财务部、人事部这样的敏感部门，其网络上的信息不想让太多人可以随便进出，于是公司采用了VLAN的方法来解决以上问题。通过VLAN的划分，可以把公司主要网络划分为：生产部、财务部、人事部和信息中心四个主要部分，对应的VLAN组名为：Product、Finance、Human、Information，各VLAN组所对应的网段如表1所示。

**表1 配置表**

|  |  |  |
| --- | --- | --- |
| VLAN号 | VLAN名 | 端口号 |
| 2 | Product | Switch1 2－23 |
| 3 | Finance | Switch2 2－15 |
| 4 | Human | Switch3 2－10 |
| 5 | Information | Switch3 11－20 |

注意：之所以把交换机的VLAN号从2号开始，那是因为交换机有一个默认的VLAN，即1号VLAN，它包括所有连在该交换机上的用户。

VLAN网络可以是有混合的网络类型设备组成，比如：10M以太网、100M以太网、令牌网、FDDI、CDDI等等，可以是工作站、服务器、集线器、网络上行主干等等。

1. **VLAN的优越性**

任何技术要得到广泛支持和应用，肯定存在一些关键优势，VLAN技术也一样，它的优势主要体现在以下几个方面：

1. 增加了网络连接的灵活性

借助VLAN技术，能将不同地点、不同网络、不同用户组合在一起，形成一个虚拟的网络环境，就像使用本地LAN一样方便、灵活、有效。VLAN可以降低移动或变更工作站地理位置的管理费用，特别是一些业务情况有经常性变动的公司使用了VLAN后，这部分管理费用大大降低。

1. 控制网络上的广播

VLAN可以提供建立防火墙的机制，防止交换网络的过量广播。使用VLAN，可以将某个交换端口或用户赋予某一个特定的VLAN组，该VLAN组可以在一个交换网中或跨接多个交换机，在一个VLAN中的广播不会送到VLAN之外。同样，相邻的端口不会收到其他VLAN产生的广播。这样可以减少广播流量，释放带宽给用户应用，减少广播的产生。

1. 增加网络的安全性

因为一个VLAN就是一个单独的广播域，VLAN之间相互隔离，这大大提高了网络的利用率，确保了网络的安全保密性。人们在LAN上经常传送一些保密的、关键性的数据。保密的数据应提供访问控制等安全手段。一个有效和容易实现的方法是将网络分成几个不同的广播组。网络管理员限制了VLAN中用户的数量，并禁止未经允许而访问VLAN中的应用。交换机的端口可以基于应用类型和访问特权来进行分组，被限制的应用程序和资源一般置于安全性VLAN中。

1. **VLAN的划分方法**

VLAN在交换机上的实现方法，可以大致划分为六类：

1. 基于端口划分VLAN

这是一种最常用、最有效的VLAN划分方法。目前绝大多数VLAN协议的交换机都提供这种配置方法。这种划分VLAN的方法是根据以太网交换机的交换端口来划分的，它是将VLAN交换机上的物理端口和VLAN交换机内部的PVC（永久虚电路）端口分成若干个组，每个组构成一个虚拟网，相当于一个独立的VLAN交换机。

当不同部门需要互访时，可通过路由器转发，并配合基于MAC地址的端口过滤。对某站点的访问路径上最靠近该站点的交换机、三层交换机或路由器的相应端口上，设定可通过的MAC地址集。这样就可以防止非法入侵者从内部盗用IP地址从其他可接入点进行网络入侵的可能。

从这种划分方法本身我们可以看出，这种划分的方法的优点是定义VLAN成员时非常简单，只要将所有的端口都定义为相应的VLAN组即可。适合于任何大小的网络。它的缺点是如果某用户离开了原来的端口，到了一个新的交换机的某个端口，必须重新定义。

1. 基于MAC地址划分VLAN

这种划分VLAN的方法是根据每个主机的MAC地址来划分，即对每个MAC地址的主机都配置他属于哪个组。它的实现机制就是每一块网卡都对应唯一的MAC地址，VLAN交换机跟踪属于VLAN MAC的地址。这种方式的VLAN允许网络用户从一个物理位置移动到另一个物理位置时，自动保留其所属VLAN的成员身份。

由这种划分的机制可以看出，这种方法的最大优点就是当用户的物理位置移动时，即从一个交换机移到其他的交换机时，VLAN不用重新配置。因为它是基于用户，而不是基于交换机端口的。这种方法的缺点是初始化时，所有的用户都必须进行配置。如果有成百上千个用户的话，配置是非常麻烦的，所以这种划分方法通常适用于小型局域网。并且这种划分的方法也导致了交换机执行效率的降低，因为在每一个交换机的端口都可能存在很多个VLAN组的成员，保存了许多用户的MAC地址，查询起来相当不容易。另外，对于使用笔记本电脑的用户来说，他们的网卡可能经常更换，这样VLAN就必须经常配置。

1. 基于网络层协议划分VLAN

VLAN按网络层协议来划分，可分为IP、IPX、DECnet、AppleTalk、Banyan等VLAN网络。这种按网络层协议来组成的VLAN可使广播域跨越多个VLAN交换机。这对于希望针对具体应用和服务来组织用户的网络管理员来说是非常具有吸引力的。而且，用户可以在网络内部自由移动，但其VLAN成员身份仍然保留不变。

这种方法的优点是用户的物理位置改变后，不需要重新配置所属的VLAN，而且可以根据协议类型来划分VLAN，这对网络管理者来说很重要。还有，这种方法不需要附加帧标签来识别VLAN，这样可以减少网络的通信量。这种方法的缺点是效率低，因为检查每一个数据包的网络层地址是需要消耗处理时间的（相对于前面两种方法），一般的交换机芯片都可以自动检查网络上数据包的以太网帧头，但要让芯片能检查IP帧头，需要更高的技术，同时也更费时。

1. 根据IP组播划分VLAN

IP组播实际上也是一种VLAN的定义，即认为一个IP组播组就是一个VLAN。这种划分的方法将VLAN扩大到了广域网，因此这种方法具有更大的灵活性，而且也很容易通过路由器进行扩展，主要适合于不在同一地理范围的局域网用户组成一个VLAN，不适合局域网，因为其效率不高。

1. 按策略划分VLAN

基于策略组成的VLAN能实现多种分配方法，包括VLAN交换机端口、MAC地址、IP地址、网络层协议等。网络管理人员可根据自己的管理模式和本单位的需求来决定选择哪种类型的VLAN。

1. 按用户定义、非用户授权划分VLAN

基于用户定义、非用户授权来划分VLAN，是指为了适应特别的VLAN网络，根据具体的网络用户的特别要求来定义和设计VLAN，而且可以让非VLAN群体用户访问VLAN，但是需要提供用户密码，在得到VLAN管理的认证后才可以加入该VLAN。

1. **基于Cisco交换机的VLAN划分**
2. 基本命令
   * show version：用来显示交换机的相关信息，包括：型号、在线时间、以太网接口个数、基本以太网地址（此地址代表交换机，在最小生成树算法中使用）。需要说明的是交换机的每一个端口都有一个MAC地址。
   * ip address IP地址 子网掩码：为交换机设置IP地址。例如：

**ip address 210.85.203.22 255.255.255.0**（回车）

为交换机的某一个端口设置IP地址后，就可以使用该地址访问和管理该交换机。

* + ip default-gateway IP地址：设置默认网关。例如：

**ip default-gateway 210.85.203.254**（回车）

* + duplex {auto | full | full-flow-control | half}：设置接口的工作模式。其参数说明如下：
    - auto：自动协商。
    - full：全双工。
    - full-flow-control：双工流控。
    - half：半双工。
  + show mac-address-table：查看MAC地址表。

另外，在特权模式下还有几个命令用来显示交换机的信息：

* + show ip：显示交换机IP地址的配置情况。
  + show running-config：列出交换机的配置清单。
  + show interface 端口：列出某个端口的具体信息。例如Cisco 1912交换机有12个以太网接口和两个快速以太网接口，显示12个以太网接口中的某一个可以用如下命令：

**show interface e0/8**（回车）

显示2个快速以太网接口中的某一个，可以使用如下命令：

**show interface fa0/26**（回车）

1. 配置命令

VLAN的配置过程非常简单，只需两步：（1）为各VLAN组命名；（2）把相应的VLAN对应到相应的交换机端口。

* + vlan vlan-id [name vlan\_name]：创建VLAN。其中：vlan-id为VLAN号，取值范围为2—1001。vlan\_name为VLAN命名的名字。例如：

(config)# **vlan 20 name Production**（回车）

此命令需要在全局模式下使用。如果需要设置多个VLAN，可以重复上述命令。创建完后用exit命令从全局模式退出保存设置。

* + vlan-membership static vlan\_id：把端口加入到指定的VLAN号。如：

|  |  |
| --- | --- |
| > **en**（回车）  # **conf t**（回车）  (config)# **vlan 20 name SXTJ**（回车）  (config)# **int e0/8**（回车）  (config-if)# **vlan-m static 20**（回车）  (config-if)# **exit**（回车）  (config)# | 进入特权模式  进入全局模式  定义VLAN20并命名为Production  进入E0/8端口  将端口静态配置到VLAN20  保存并返回到特权模式 |

1. 实例

下面通过一个具体实例说明如何使用Cisco交换机进行VLAN划分。该实例的拓扑图如图2所示：

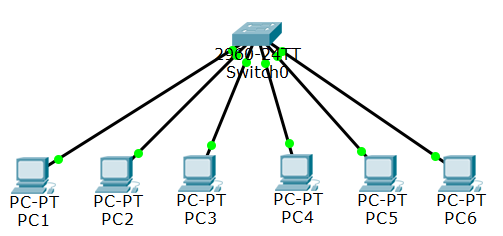


图2 VLAN配置实例

图2中各PC机的IP地址、掩码、端口、VLAN编号和默认网关配置如表2：

**表2 VLAN的配置表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 设备 | IP地址 | 掩码 | 默认网关 | 交换机端口 | VLAN编号 |
| PC1 | 172.16.21.11 | 255.255.255.0 | 172.16.21.1 | Ethernet 0/1 | 1 |
| PC2 | 172.16.21.12 | 255.255.255.0 | 172.16.21.1 | Ethernet 0/2 | 1 |
| PC3 | 172.16.21.13 | 255.255.255.0 | 172.16.21.1 | Ethernet 0/3 | 1 |
| PC4 | 172.16.21.14 | 255.255.255.0 | 172.16.21.1 | Ethernet 0/4 | 2 |
| PC5 | 172.16.21.15 | 255.255.255.0 | 172.16.21.1 | Ethernet 0/5 | 2 |
| PC6 | 172.16.21.16 | 255.255.255.0 | 172.16.21.1 | Ethernet 0/6 | 2 |

具体配置步骤如下：

Step 1：配置PC1的IP地址和默认网关。命令如下：

|  |  |
| --- | --- |
| C:> **ipconfig /ip 172.16.21.11 255.255.255.0**（回车）  C:> **ipconfig /dg 172.16.21.1**（回车） | 设置IP地址和子网掩码  设置默认网关 |

采用类似的方法设置PC2到PC6的IP地址、子网掩码和默认网关，其参数值如表2。

Step 2：设置交换机：

|  |  |
| --- | --- |
| > **en**（回车）  # **conf t**（回车）  (config)# **hostname SXTJ**（回车）  XXJS(config)# **vlan 1 name SXTJ1**（回车）  XXJS(config)# **vlan 2 name SXTJ2**（回车）  XXJS(config)# **int e0/4**（回车）  XXJS(config-if)# **vlan-m static 2**（回车）  XXJS(config-if)# **exit**（回车）  XXJS(config)# **int e0/5**（回车）  XXJS(config-if)# **vlan-m static 2**（回车）  XXJS(config-if)# **exit**（回车）  XXJS(config)# **int e0/6**（回车）  XXJS(config-if)# **vlan-m static 2**（回车）  XXJS(config-if)# **exit**（回车） | 进入特权模式  进入全局模式  配置主机名字为SXTJ  定义vlan1并命名为SXTJ1  定义vlan2并命名为SXTJ2  进入e0/4端口  将端口配置到XXJS2  保存并返回全局模式  进入e0/4端口  将端口配置到XXJS2  保存并返回全局模式  进入e0/4端口  将端口配置到XXJS2  保存并返回全局模式 |

配置结束后，可以在特权模式下察看某个VLAN的有关信息，命令如下：

|  |  |
| --- | --- |
| XXJS# **show mac-address-table**（回车）  XXJS# **show vlan 1**（回车） | 显示MAC信息表  显示XXJS1组的有关信息 |

同学也可以尝试采用图形方式进行VLAN设置，具体操作方法，请同学们自行尝试，如图3所示：

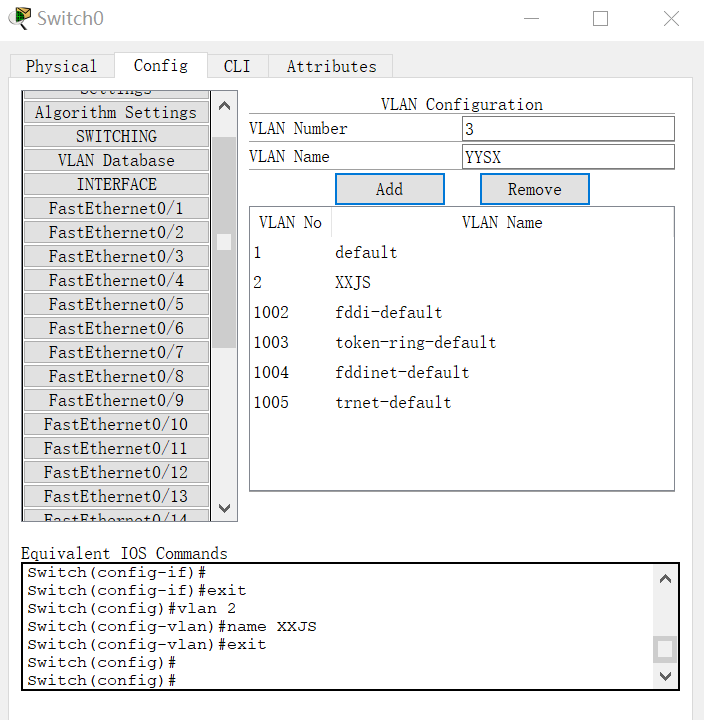


图3 VLAN的图形化配置

当察看并确认没有错误之后，使用ping命令在PC机上测试各VLAN计算机中的连通性。具体操作过程见实验二的相关内容。

三、实验任务

按照图4所示的网络拓扑图进行VLAN的配置。各PC的配置要求如表3：

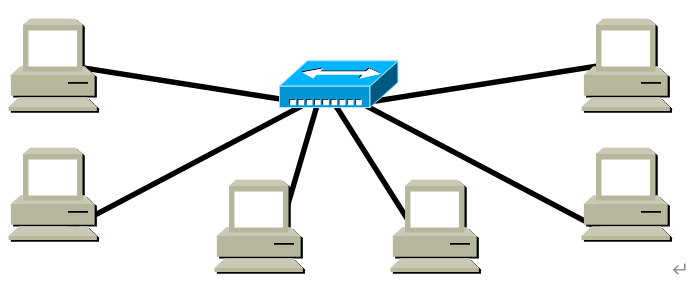
****

图4 实验用图

**表3 实验内容的各PC机的配置表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 设备 | IP地址 | 掩码 | 默认网关 | 交换机端口 | VLAN编号 |
| PC1 | 172.16.21.11 | 255.255.255.0 | 172.16.21.1 | Ethernet 0/1 | 1 |
| PC2 | 172.16.21.12 | 255.255.255.0 | 172.16.21.1 | Ethernet 0/2 | 2 |
| PC3 | 172.16.21.13 | 255.255.255.0 | 172.16.21.1 | Ethernet 0/3 | 3 |
| PC4 | 172.16.21.14 | 255.255.255.0 | 172.16.21.1 | Ethernet 0/8 | 1 |
| PC5 | 172.16.21.15 | 255.255.255.0 | 172.16.21.1 | Ethernet 0/9 | 2 |
| PC6 | 172.16.21.16 | 255.255.255.0 | 172.16.21.1 | Ethernet 0/10 | 3 |

1. 实验所需要的设备

模拟软件中的Cisco交换机1个、PC机6台。

1. 实验步骤
2. 在模拟器中设置相应设备，并用合适的连接线进行连接。
3. 使用命令以及图形方式进行相应设备的网络接口配置。
4. 实验的验证方式

在PC1机上用ping到其他各PC。记下屏幕截图或命令执行时屏幕上显示的内容。并使用Simulation Mode模式观测ping命令中的ICMP报文包转发过程。

四、实验思考

为什么要使用虚拟局域网？它有什么好处？