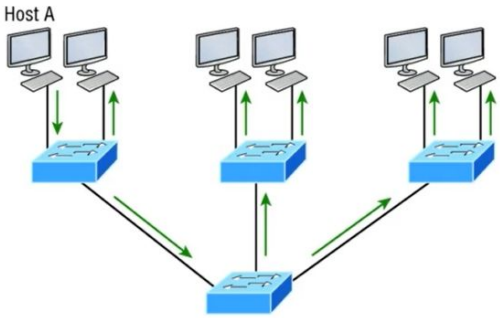
计算机网络工程
2020 学年上学期

李述兴
hingsmy@gmail.com

2020 年 11 月 2 日 第8周

Virtual LAN (VLAN) Basic 虚拟局域网（VLAN）基础

A group of devices within a VLAN communicate as if they were attached to the same wire. VLANs are based on logical connections, instead of physical connections. VLAN中的一组设备进行通信，就像它们连接到同一条线上一样。VLAN基于逻辑上的连接，而不是物理上的连接。



Flat network - one broadcast domain 扁平网络 - 一个广播域

- Logical segregation 逻辑上的隔离
- Enhance network security 增强网络安全性
- Increase the number of broadcast domains while decreasing their size 增加广播域的数量，同时减小其大小

Ethernet VLANs 1 and 1006 through 4094 use only default values. 以太网VLAN 1和1006至4094仅使用默认值。

---

vlan的英文是virtual lan缩写，中文即虚拟的局域网。

为什么我们需要用到vlan这种技术？在vlan出现之前，所有的交换机连接在一起，那么它们形成了一个单一平面的网络架构。交换机在默认情况下，一个交换机就是一个broadcast domain，交换机直连过后，它形成的也是一个broadcast domain。

一个broadcast domain给我们带来了哪些问题？

第一，一个广播域里面，如果其中一台终端出问题，这台终端发出了很多广播的数据，在一个广播域里面，这些广播会转发到所有的接口。即一台终端出问题，其他的终端全部都会被影响到。随着网络越变越大，交换机越来越多，广播域也会越来越来大。随着广播域的增大，其中一台终端出问题，那么他影响到的区域也就越大。

在我们做网络设计的时候，我们会尽量的减小我们的广播域，从而我们就减小了受影响的区域。

在没有vlan的情况下，我们没有办法把广播域进行减小，因为所有的交换机连在一起，它形成了一个单一的广播域。

第二，就是安全的问题，在单一广播域，在一个flat network的情况下，比如有三个部门A、B、C，他们互相之间是可以随意访问的。每个部门他们都可以看到另外一个部门的终端，这就带来了安全和管理上的问题。正是为了解决这些问题，我们有了vlan虚拟局域网这种技术，

它的概念是什么呢？他就是在同一台物理的交换机上面，虚拟出多个局域网，每一个局域网我用一个数字来表示，那么我们就称它为vlan ID。这个数字，比如vlan1 vlan2 vlan3 ，一个vlan Id就代表了一个虚拟出来的局域网。

比如说现在我这边有两个部门，一个是sales，一个是admin。我把sales部门的这两台电脑放进一个vlan，那么我把admin的这两台电脑放进另一个vlan，它们相互之间是看不见对方的，而且也无法进行通信，就相当于他们分别连接到两个物理机一样。

那么通过这种vlan的技术，我们就把一个物理机虚拟成了很多个不同的物理交换机，虚拟成了很多个不同的交换机，从而创建出了很多个广播域。

vlan带来的好处有哪些呢？第一个就是 logical segregation，就是在逻辑上，我们把它同样一台物理交换机给分割开来的，通过了这种逻辑上的分割，我们就增强了安全，也方便了管理。分割之后，不同vlan之间，默认情况下是无法进行相互通信的。同时由于我们对整个一个大的局域网来进行了分割，我们创造出了更多的广播域。

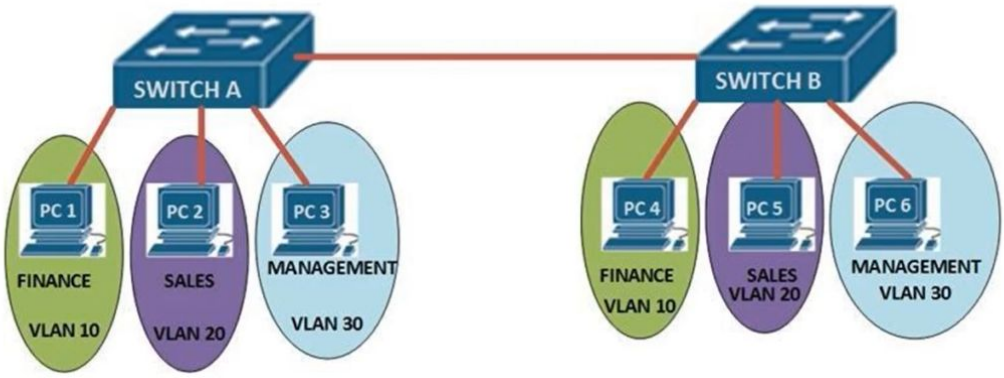
在没有virtual lan的概念下，一个局域网是一个广播域，而当我们用vlan这种技术对lan进行分割过后，我们就创建出了两个vlan。虽说我们的广播域的数量有所增加，可是每一个广播域它的大小是减小了，这就意味着我们把可能出现问题的区域影响的范围也减小了。

这个时候如果hostA出问题，那么它影响的将只会是 sales vlan里面的hostB，这是因为sales vlan跟我们的admin vlan它之间不可以进行通信，所以 sales vlan出问题，那么不会影响到我们的admin vlan，那么这就是vlan带来的一些好处。

在一个物理交换机上，vlan ID是从1~4094，其中 vlan1 它是一个默认的vlan，当开启一个交换机的时候，所有的端口它默认在vlan1下面。vlan 1006到4096，是已经被系统内部预定的，我们没

有办法对1006~4096这个范围里的vlan进行任何的修改。实际上我们可以人为创建和修改的vlan是从2开始一直到1005。

Access and Trunk Port 接入和中继端口



Access Port 接入端口

- Belongs to and carries the traffic of only one VLAN 属于并且仅携带一个VLAN的流量
- Traffic is both received and sent in native formats with **no VLAN information (tagging)** whatsoever 流量以本地格式接收和发送，**没有任何VLAN信息（标记）**

Trunk Port 中继端口

- Carries the traffic of multiple VLANs 携带多个VLAN的流量

在图中的拓扑里有两台交换机，每一台交换机上我都连接了三个不同部门的 PC，那么有finance、sales、management，为了能够让同一个部门之间的电脑进行通信，而不同部门的电脑不能够互相通信，我们就创建出三个vlan，给finance创建了一个vlan10 ，给sales创建了一个vlan20，给management创建了一个vlan30。

在交换机上面，当我们创建完vlan之后，我们需要把交换机连接 PC的端口，把它放在相应的vlan下面，把它做一个映射，比如说第一个端口它是属于vlan10的，第二个端口是属于vlan20的，第三个端口是属于vlan30的。这种用来连接我们的终端PC的这种端口，有一个名称叫做access port。

access port 它有两个很特别的属性，第一个就是access port一定是对应一个vlan，而且它也只能对应一个vlan，他只能携带单一vlan的流量。第二个属性，access port收到的和发出的数据包都是没有做vlan tagging的，都是没有打上标签的。

比如我在交换机上我创建了一个vlan10，当你的电脑往交换机发送数据的时候，这个数据里面不会有相应的vlan的信息。当数据被交换机接收到以后，交换机通过查看我这个端口和vlan ID之间的映射，交换机才会知道你这个数据包是属于哪一个vlan的，

在这个过程当中，交换机接收到的数据包，或者是从PC发送出去的数据包，是没有做vlan tagging的，没有打上vlan的标签的。即数据包本身是不知道它是属于什么vlan的，只有当它到了交换机端口以后，交换机通过查看配置发现这个端口跟其中某一个vlan有一个映射关系，交换机才会知道这个数据包是属于该vlan。

交换机发送给我们电脑的数据包，它同样也是没有打标签的。

还有一种端口模式，我们叫做trunk port，trunk port是用来做什么？trunk port carries the traffic of multiple vlan，也就是说trunk port，它的用处是当你需要多个vlan的数据流量通过的时候，我们就要用trunk port，比如说如图中，我的switchA跟switchB中间的这两个接口，就要用trunk port。

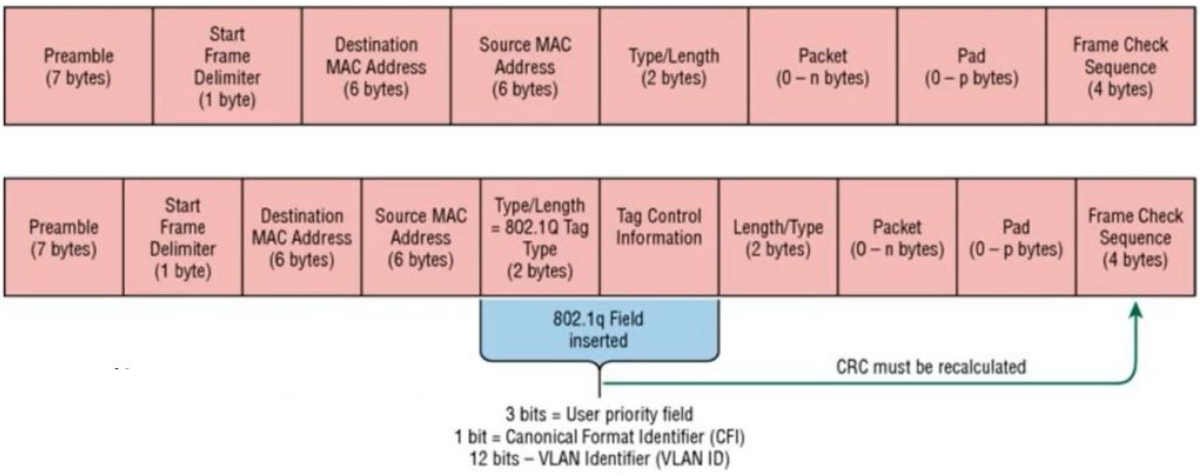
因为我左边有三个vlan，我这三个vlan要对应发送数据到右边的这三个vlan里面去。那么在这条链路上，我的数据包就会出现三种vlan的数据包。为了区分这些数据包，当我的数据包从我们的trunk port发送出去的时候，这个时候需要打上标签，发送出去这个数据包，要把它打上标签，比如说vlan10、vlan20、vlan30。接收端我看到了这些标签才知道怎么把这些数据转发到对应的access port上面。

比如我收到一个数据包，上面的标签是10，通过查看switchB的配置，我知道第一个端口是vlan10下面，那么我这个数据包就会转发到 PC4上面。

在一般情况下，我们的交换机与交换机之间连接用trunk port，交换机和终端连接，一般情况下我们用access port。

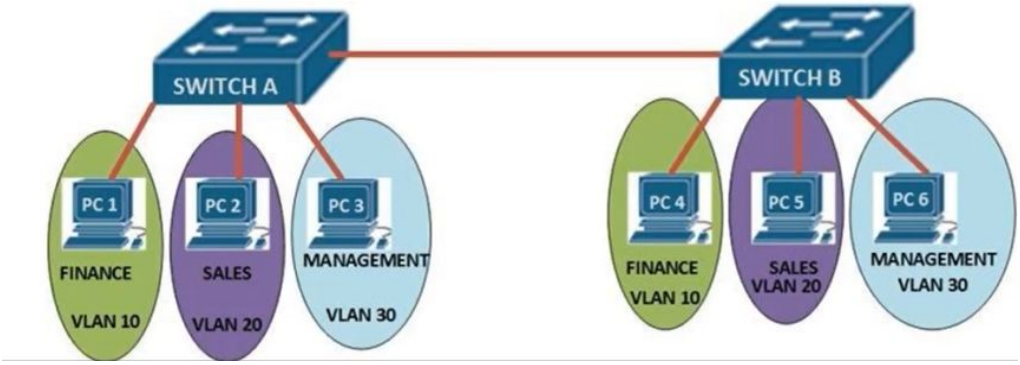
特殊情况比如说，当网络里面只有一个vlan的时候，交换机和交换机之间可以用assess port。交换机连接我的终端的时候，比如说你连接的是一个服务器，而这个服务器上面跑了很多vm ，当我有一个服务器上面在跑vm的时候，这个服务器端口可以把它配置成一个trunk。在这个服务器内部可以创建很多个vlan这种情况下，交换机虽然看起来它连接的是一个终端，但在这个服务器里面，它有很多不一样的vlan，所以我的交换机端口也要用trunk。

Frame Tagging 帧标签



- Inter-Switch Link(ISL)
- IEEE 802.1q

802.1q tagged frame can carry information for 4094 VLANs (2^{12}) 802.1q标记的帧可以携带4094个VLAN的信息（2^{12}）



trunk是通过一些协议实现的。我们有两种办法去配置trunk，一种是把trunk配置成ISL，另外一种是把trunk配置成802.1q。ISL这种封装的模式为思科私有，所以没有人用。

我们现在能够看到的都是用的802.1q这种格式来做vlan tagging 来打标签打上vlan ID。

图一上面的这种数据帧的格式就是ISL，下面这种数据帧是802.1q的。

vlan的数量是从1~4094的原因，是因为插入位置的比特数的原因，只有12个比特用来存放的vlanID，所以就是2的12个次方，所以我们一共有409 4个vlan。

通过实验学习配置Access Port和Trunk Port。