# 802.10 的 VLAN 协议与技术

刘玲　胡楠　（南京经济学院信息中心　210003）

## 1.802.10 的 VLAN 协议特性

今日的网络在物理 LAN 的基础上依据工作组进行 VLAN 的划分，VLAN 隔离了广播风暴，提供了有效的带宽使用，使得数据包只在归属于同一个 VLAN 的端口转发，由于缺乏有效的 VLAN 的标准，导致了 VLAN 广泛应用的某种限制，为实现跨越 FDDI 的高速连接划分 VLAN，我们采用 802.10 的 VLAN 协议。

802.10 VLAN 协议采用了增加 VLAN 标识符的机制，保证依据标识符数据包作有选择的传输，802.10 VLAN 协议源于基于 LAN/MAN 互通 SILS 安全标准，SILS 最初是为解决共享局域网和城域网的安全问题提出，于 1992 年被国际认可，他集成了认证和秘钥技术确保数据的可靠性和跨越网络的完整性，此外，由于此标准作用于 OSI 模型的第二层，所以特别适合于要求高直通低延时的交换环境。

802.10 标准定义了一个单一协议控制单元 PDU (Protocol DataUnit)，我们称为数据安全交换（Secure Data Exchange SDU)PDU，这是一个在 MAC 包头和数据帧之间加插了 802.10 包头的 MAC 层帧(即第二层。)，其中 802.10 的包头有内外两个包头组成，分别称之为 Clear Header 和 Protected Header，具体如 Figure 1。

Figure 1:802.10 Header

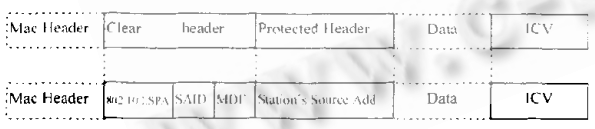


图 1

如上所示，Clear Header 包括与安全有关的标识 SAID 和可选的管理定义单元 MDF，MDF 可用于简化 PDU 的处理，802.10 LSPA 用于表明数据包为 802.10 VLAN 帧格式。而 Protected Header 复制 Mac Header 中的源地址作为地址确认，这样一来可以防止其他的终端站被当作源站。ICV 负责集成数据检查，使用一种安全算法技术防止对包内携带数据的非授权修改。此外，对于 802.10 包头的每一个部分，均有一可选择的秘钥，用以保证跨越共享媒体介质实现数据传输的安全，通过 802.10 协议和 SMIB(Security Management Information Base)的结合，任何 LAN 设备均能获得一个 SAID 标识和一个秘匙，使得数据只在具相同安全需求的团体之间进行交换，如局限在一个部门内。

当把 802.10 与 VLAN 相关时，VLAN 的 ID 号变为至关重要，此时 802.10 的 SAID 区被用于 VLAN 的 ID，通过这个标识可以判断通信属于哪个特定的 VLAN，更进一步，互联设备将判断互联网上哪一个 VLAN 归口在哪一个端口。这样一来数据只会在同一 VLAN 内部广播，隔离了广播风暴。

因为建立 VLAN 的最主要的目的是为了跨越物理上的界限，而不是在传输数据中加载秘匙而导致因解密算法而造成的执行性能的降低。所以只要求高连通设备必须支持 Figure 1 中的 Clear header 部分，在实际划分 VLAN 时，802.10 的包头只包含 SDE DESIGNATOR，即 Figure 1 中的 802.10 LSPA（表明为 802.10 的 VLAN）和 VLAN ID(SAID) 这两部分。这两部分一共占七个字节，其中 SAID 占用 4 个字节，所以他能表示的 VLAN 是相当多的。

## 2.802.10 如何工作?

基于 LAN 子网划分 VLAN 之后，任何终端站发送的数据包均获得一个 802.10 的包头，其中包含此 VLAN 的 ID 号，这个数据包只广播给同一 VLAN 组中的成员，而不作全网广播，当然，这个动作的完成需要主干网上的其他网络设备的配合(如交换机、路由器)，接受到数据包的这些设备进行 VLAN ID 号的匹配比较，那些 ID 号与任何设备端口不匹配的数据包将被过滤掉，而那些与某一端口匹配的数据包将被剥除 802.10 部分之后将原始数据包转发到相应的属于同一 VLAN 的端口，因为 802.10 的 VLAN 数据包为合法的 MAC 帧，所以他们可以被非 802.10 兼容的设备转发或传输，此外直接挂接在 FDDI、Ethernet、Token Ring 主干的服务器也可以采用

VLAN ID 同时接入一个或数个 VLAN，以实现跨 VLAN 的资源共享。以上可表示为如图 2 所示。以 Ethernet 或 FAST Ethernet 挂接在传统 Switch Hub 上并被 FDDI 分割的工作站可以化

Figure 2


图 2

归为同一个 VLAN，且共享网络资源（文件打印 Email 服务器）不需要 Router 的前提下，跨越多个 VLAN，即多个 VLAN 上的用户可以同时访问到共享资源。

VLAN 对于今日网络分段要求提供了一个高灵活性可扩充性的解决方案。而 802.10 标准提供划分 VLAN 机制的同时融合了全面的安全特征，这正是今日共享网络环境的要求，而且基于 802.10 和 ISL 技术加之 LAN Emulation 划分的 VLAN 可以将 FDDI、Fast Ethernet 、ATM 甚至端到端的串口连接分开的终端站划归为一个 VLAN，实现共享资源跨越多个 VLAN，在保留现有网络结构的基础上实现 VLAN 划分，不仅保护了用户的投资，也便于将来的网络升迁。

（来稿时间：1997 年 9 月）