

项目二：知识链接

1.1.1 知识链接

1. 交换技术

局域网交换技术是在传统的以太网技术的基础上发展而来，随着局域网范围的扩大和网络通信技术的发展，目前在企业网络中以太网交换技术是网络发展中非常活跃的部分，交换技术在局域网中处于非常重要的地位。

局域网交换技术是 OSI 参考模型中的第二层——数据链路层（Data- Link Layer）上的技术，所谓“交换”实际上就是指转发数据帧（frame）。实现交换技术的网络设备就是以太网交换机（Switch）。

2. 虚拟局域网（VLAN）

VLAN（Virtual Local Area Network）即虚拟局域网，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，这些网段内的机器有着共同的需求而与物理位置无关（如图 3-2 所示）。IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 802.1Q 协议标准草案。

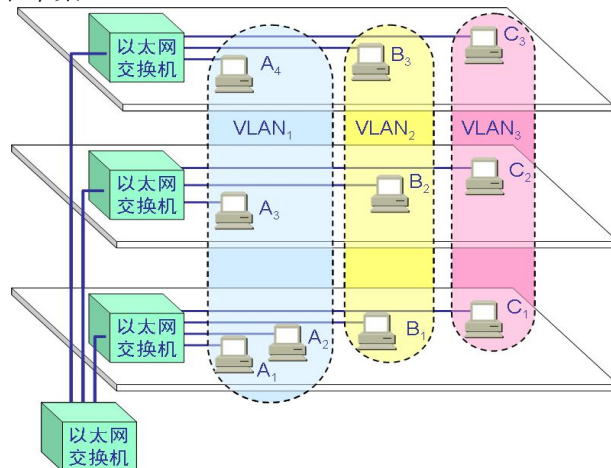


图 1-1 VLAN 结构示意图

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，每一个 VLAN 都有一个明确的标识符即 VLAN ID 号，限制不同工作组间的用户二层互访，每个工作组就是一个虚拟局域网。虚拟局域网的好处是可以限制广播范围，并能够形成虚拟工作组，动态管理网络，并能进一步结合 IP 技术实现三层交换功能。

VLAN 其实只是局域网给用户提供服务的一种服务，对于用户而言是透明的，并不是一种新型的局域网。

3. Vlan trunk

VLAN Trunk 即虚拟局域网中继技术。其功能是让连接在不同交换机上的相同 VLAN 中的主机互通。和级联技术相对应。按照级联技术来讲：如果在 2 个交换机上分别划分了多个 VLAN，那么分别在两个交换机上的相同 VLAN 内部的成员如果要相互通信，级联的做法是，需要在两个交换机上用一根级联线连接相同 VLAN。也就是说如果交换机上划分多个 VLAN，那么就要连接相应数量的线作为级联线。显然，使用级联技术端口使用效率太低，也不现实。因此 VLAN TRUNK 技术应运而生，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 VLAN 也只用 1 个端口就解决了。

Tag VLAN 成员端口间通信。802.1Q 协议使跨交换机的相同 VLAN 里端口间通信成为可能，Tag VLAN 用 VID 来划分不同的 VLAN。当数据帧通过交换机的时候，交换机根据帧中 TAG 头的 VID 信息来识别它们所在的 VLAN（但是若帧中无 TAG 头，则应用帧所通过端口的缺省 VID 信息来识别它们所在的 VLAN），这使得所有属于该 VLAN 的数据帧，都将限制在该逻辑 VLAN 中传播这将使组中主机之间能够相互彼此通信，而不受其它主机的影响，就像它们存在于单独的 VLAN 当中一样。如图 1-8 所示：

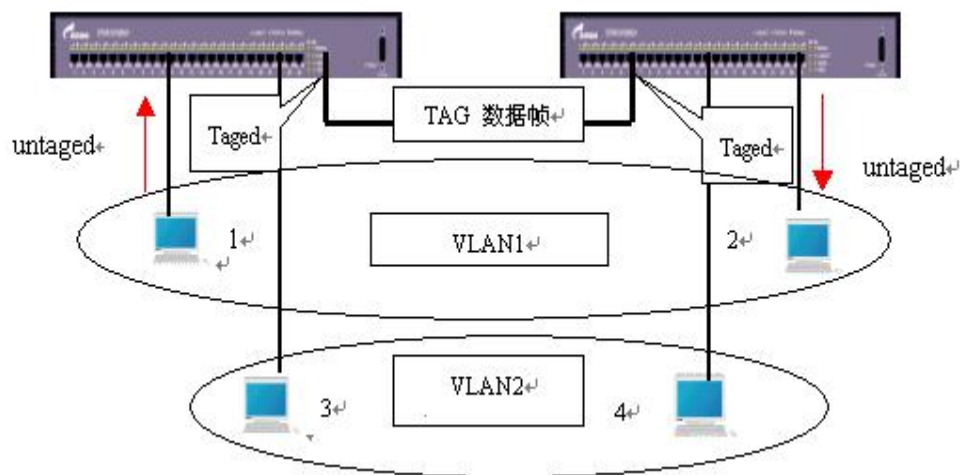


图 1-2 Tag VLAN 成员端口通信示意图

4. 单臂路由技术

单臂路由（router-on-a-stick）是指在路由器的一个接口上通过配置子接口（或“逻辑接口”，并不存在真正物理接口）的方式，实现原来相互隔离的不同 VLAN（虚拟局域网）之间的互联互通。

单臂路由的子接口

路由器的物理接口可以被划分成多个逻辑接口，这些被划分后的逻辑接口被形象的称为子接口。值得注意的是这些逻辑子接口不能被单独的开启或关闭，也就是说，当物理接口被开启或关闭时，所有的该接口的子接口也随之被开启或关闭。

优缺点

VLAN 能有效分割局域网，实现各网络区域之间的访问控制。但现实中，往往需要配置某些 VLAN 之间的互联互通。比如，你的公司划分为领导层、销售部、财务部、人力部、科技部、审计部，并为不同部门配置了不同的 VLAN，部门之间不能相互访问，有效保证了各部门的信息安全。但经常出现领导层需要跨越 VLAN 访问其他各个部门，这个功能就由单臂路由来实现。

优点：实现不同 vlan 之间的通信，有助理解、学习 VLAN 原理和子接口概念。

缺点：容易成为网络单点故障，配置稍有复杂，现实意义不大。

单臂路由实现原理如下图所示。

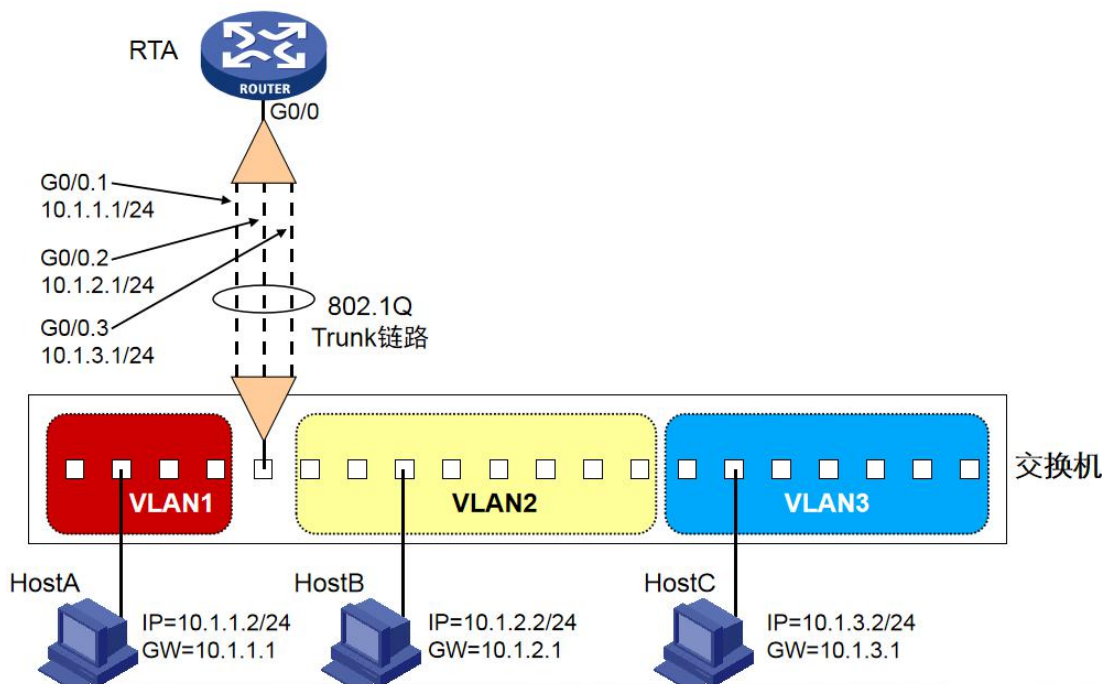


图 1-3 单臂路由实现原理

5. telnet

1. 概述

Telnet 协议是 TCP/IP 协议族中的一员，是 Internet 远程登陆服务的标准协议。Telnet 协议的目的是提供一个相对通用的，双向的，面向八位字节的通信方法，允许界面终端设备和面向终端的过程能通过一个标准过程进行互相交互。应用 Telnet 协议能够把本地用户所使用的计算机变成远程主机系统的一个终端。

在分布式计算环境中，常常需要调用远程计算机的资源同本地计算机协同工作，这样就可以用多台计算机来共同完成一个较大的任务。这种协同操作的工作方式就要求用户能够登录到远程计算机中去启动某个进程，并使进程之间能够相互通信。为了达到这种目的，人们开发了远程终端协议，即 Telnet（Telecommunications Network Protocol）协议。Telnet 协议是 TCP/IP 协议的一部分，它精确地定义了远程登录客户机与远程登录服务器之间的交互过程。Telnet 给用户提供了一种通过其连网的终端登录远程服务器的方式。Telnet 使用的传输层协议为 TCP，使用端口号 23。Telnet 要求有一个 telnet 服务器程序，此服务器程序通常驻留在主机上。客户端通过运行 Telnet 客户端程序远程登录到 Telnet 服务器来实现资源共享。

当用户通过客户端向 Telnet 服务器发出上网登录请求后，Telnet 服务器将返回一个信号，要求本地用户输入自己的登录名（Login Name）和口令（Password），只有用户返回的登录名与口令正确，登录才能成功。在 Internet 上，很多主机同时装载有寻求服务的程序和提供服务的程序，也就是既可以作为客户端，也可以作为 Telnet 服务器使用。如图 6-17 所示。

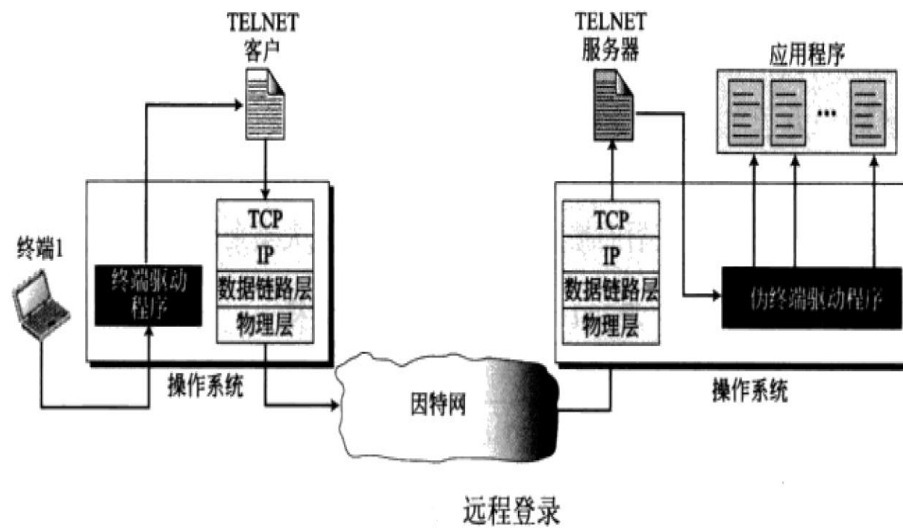


图 1-4 Telnet 工作原理

➤ 提示：Telnet 在传输过程中使用明文，为了防止远程管理过程中的信息泄露问题，常使用具有加密功能的 SSH（Secure Shell）。