 交换机不是被设计用来作安全设备的，其功能仍是以提高网络性能为主。如果要将交换机纳入安全机制的一部分，前提是首先要对交换机进行正确的配置，其次交换机的制造商要对交换机软件的基础标准有着全面理解并彻底实现了这些标准。 如果对网络安全有着严格的要求，还是不要使用共享的交换机，应该使用专门的交换机来保证网络安全。如果一定要在不可信的网络和可信的用户之间共享一个交换机，那么带来的只能是安全上的灾难。 VLAN的确使得将网络业务进行隔离成为可能，这些业务共享同一交换机甚至共享一组交换机。但是交换机的设计者们在把这种隔离功能加入到产品之中时，优先考虑的并不是安全问题。VLAN的工作原理是限制和过滤广播业务流量，不幸的是，VLAN是依靠软件和配置机制而不是通过硬件来完成这一任务的。 最近几年，一些防火墙已经成为VLAN设备，这意味着可以制定基于包标签的规则来使一个数据包转到特定的VLAN。然而，作为VLAN设备的防火墙也为网页寄存站点增加了很多灵活的规则，这样防火墙所依赖的这些标签在设计时就不是以安全为准则了。交换机之外的设备也可以生成标签，这些标签可以被轻易地附加在数据包上用来欺骗防火墙。 VLAN的工作原理究竟是怎样的？VLAN又有着什么样的安全性上的优点呢？如果决定使用VLAN作为安全体系的一部分，怎样才能最大限度地避免VLAN的弱点呢？ 分区功能“ 交换机 ”一词最早被用来描

述这样一种设备，这种设备将网络业务在被称之为“ 端口 ”的网络接口间进行交换。就在不久以前，局域网的交换机被称作“ 桥接器 ”。现在，即使是与交换机相关的IEEE标准中也不可避免地用到“ 桥接器 ”这一术语。 桥接器用来连接同一局域网上不同的段，这里的局域网指的是不需要路由的本地网络。桥接器软件通过检测收到数据包中所含的MAC地址来获悉哪个端口联接到哪个网络设备。最初，桥接器将所有收到的数据包发送到每个端口，经过一段时间以后，桥接器通过建立生成树和表的方法获悉如何将数据包发送到正确的网络接口。这些生成树和表将MAC地址映射到端口的工作，是通过一些选择正确网络接口和避免回路的算法来完成的。通过将数据包发送到正确的网络接口，桥接器减少了网络业务流量。可以将桥接器看作是连接两条不同道路的高速公路，在高速公路上只通过两条道路间必要的交通流量。 尽管桥接器从整体上减少了网络业务流量，使得网络可以更加高效地运行。桥接器仍然需要对所有端口进行广播数据包的发送。在任何局域网中，广播的含义是：一个消息广播发送给局域网内所有系统。ARP（地址解析协议）包就是广播信息的一个例子。 随着端口数目和附加管理软件数目的增多，桥接器设备的功能变得越来越强。一种新的功能出现了：桥接器具有了分区功能，可被分成多个虚拟桥。当通过这种方式进行分区时，广播信息将被限制在与虚拟桥和对应的VLAN的那些端口上，而不是被发送到所有的端口。 将广播限制在一个VLAN中并不能够阻止一个VLAN中的系统访问与之连接在同一桥接器而属于不同VLAN的系统。但要记住，ARP广播被用来获得与特定IP对应的MAC地址，而没有MAC地址，即使

在同一网络中的机器也不能相互通信。 Cisco网站上描述了在两种情况下，数据包可以在连接于同一交换机的VLAN中传送。在第一种情况下，系统在同一VLAN中建立了TCP/IP连接，然后交换机被重新设置，使得一个交换机的端口属于另一个VLAN。通信仍将继续，因为通信双方在自己的ARP缓冲区中都有对方的MAC地址，这样桥接器知道目的MAC地址指向哪个端口。在第二种情况下，某人希望手动配制VLAN，为要访问的系统建立静态ARP项。这要求他知道目标系统的MAC地址，也许需要在物理上直接访问目标系统。 这两种情况中所描述的问题能够通过使用交换机软件来得到改善，这些软件的功能是消除数据包在传送时所需要的信息。
在Cisco的高端交换机中，将每个VLAN所存在的生成树进行分离。其他的交换机要么具有类似的特点，要么能被设置成可以对各个VLAN里的成员的桥接信息进行过滤。 链路聚合多个交换机可以通过配制机制和在交换机间交换数据包的标签来共享同一VLAN。你可以设置一个交换机，使得其中一个端口成为链路，在链路上可以为任何VLAN传送数据包。
当数据包在交换机之间传递时，每个数据包被加上基于802.1Q协议的标签，802.1Q协议是为在桥接器间传送数据包而设立的IEEE标准。接收交换机消除数据包的标签，并将数据包发送到正确的端口，或在数据包是广播包的情况下发送到正确的VLAN。 这些四字节长的802.1Q被附加在以太网数据包头中，紧跟在源地址后。前两个字节包含81 00，是802.1Q标签协议类型。后两个字节包含一个可能的优先级，一个标志和12比特的VID（VLAN Identifier）。VID的取值在0到4095之间，而0和4095都作为保留值。VID的默认值为1

，这个值同时也是为VLAN配置的交换机的未指定端口的默认值。 根据Cisco交换机的默认配置，链路聚合是推荐的配置。如果一个端口发现另一个交换机也连在这个端口上，此端口可以对链路聚合进行协商。默认的链路端口属于VLAN1，这个VLAN被称作该端口的本地VLAN。管理员能够将链路端口指定给任何VLAN。 可以通过设置链路端口来防止这种VLAN间数据包的传送，将链路端口的本地VLAN设置成不同于其他任何VLAN的VID。记住链路端口的默认本地VLAN是VID 1。可以选择将链路端口的本地VLAN设置为1001，或者任何交换机允许的且不被其他任何VLAN所使用的值。 防火墙和VLAN 知道了交换机如何共享VLAN信息之后，就可以更准确地评价支持VLAN的防火墙。支持VLAN的防火墙从支持VLAN的交换机那里获得头部带有802.1Q标签的数据包，这些标签将被防火墙展开，然后用来进行安全规则的检测。尽管到目前为止，我们只讨论了以太网的情况，802.1Q标签同样适用于其他类型的网络，比如ATM 和FDDI。 802.1Q标签并不能提供身份验证，它们只不过是交换机用来标志从特定VLAN来的特定数据包的一种方式。如同许多年来人们伪造IP源地址一样，VLAN标签同样可以被伪造。最新的Linux操作系统带有对工作于VLAN交换机模式的支持，可以生成本地系统管理员可以选择的任意VLAN标签。 安全使用802.1Q标签的关键在于设计这样一种网络：交换机链路连接到防火墙接口，而基于VLAN标签的安全检测将在防火墙接口进行。如果有其他的线路能够到达防火墙的接口，伪造VLAN标签的可能性就会增大。交换机本身必须被正确配置，进行链路聚合的链路端口要进行特殊配置，然后加入到

非默认VID中。 在任何关于交换机的讨论中，保护对交换机设备的管理权限这一结论是永远不变的。交换机和其他网络设备一样可以从三种途径进行管理：Telnet、HTTP和SNMP。关掉不使用的管理途径，在所使用的管理途径上也要加上访问控制。因为当攻击者来自网络外部时，防火墙可以控制他对交换机的访问；当攻击者来自网络内部或者攻击者获得了访问内部系统的权限而发起攻击时，防火墙对此将无能为力。 