用VLAN解决宿舍网络安全问题 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/290/2021_2022__E7_94_A8VLAN_E8_A7_A3_c101_290886.htm 大学宿舍网络的管理可以评定为“ 最难管理的网络 ”之一。有些用户安装ARP防火墙，开启主动防御，且设置了较大的值，这样网络被大量的无用ARP 数据包占据。另外一个现象，很多用户没有安装杀毒软件或者没有及时升级，计算机被病毒感染后，向网络发送大量的病毒包。在交换机性能不变的情况下，数据包转发量恒定，ARP 包和病毒包多了，有效数据包就少了，所以网络的传输速度就明显慢了下来，且过多的无用数据包还会导致交换机性能的下降? 分析：Private VLAN技术 Private VLAN是工作在第二层的网络技术。在Private VLAN的概念中，交换机端口有三种类型：Isolated port，Community port, Promiscuous port。 它们分别对应不同的VLAN类型：Isolated port属于Isolated PVLAN，Community port属于Community PVLAN，而代表一个Private VLAN整体的是Primary VLAN，前面两类VLAN需要和它绑定在一起，同时它还包括Promiscuous port。在Isolated PVLAN中，Isolated port只能和Promiscuous port通信，彼此不能交换流量。 在Community PVLAN中，Community port不仅可以和Promiscuous port通信，而且彼此也可以交换流量。Promiscuous port 与路由器或第3层交换机接口相连，它收到的流量可以发往Isolated port和Community port。 PVLAN的应用对于保证接入网络的数据通信的安全性是非常有效的，用户只需与自己的默认网关连接，一个PVLAN不需要多个VLAN和IP子网就提供了具备第2层数据

通信安全性的连接，所有的用户都接入PVLAN，从而实现了所有用户与默认网关的连接，而与PVLAN内的其他用户没有任何访问。PVLAN功能可以保证同一个VLAN中的各个端口相互之间不能通信，但可以穿过Trunk端口。这样即使同一VLAN中的用户，相互之间也不会受到广播的影响。 在思科高端Cisco 6000和Cisco 4000 系列交换机上可以配置私有vlan，但在华为的一些低端产品上就提供了此项功能。 深入：配置PVLAN的步骤 配置PVLAN的步骤包括：配置Primary VLAN、配置Secondary VLAN、设置Primary VLAN和Secondary VLAN间的映射关系，以上任务都是必选的，一旦启用PVLAN就必须配置。具体配置命令参考下面的建议。 （1）设置VTP的transparent（透明）模式 COS交换机 set vtp mode transparent IOS交换机 （privileged） vlan database （vlan_database） vtp transparent 在创建一个私用VLAN之前，您必须配置VTP为transparent（透明）模式。私用VLAN必须在单台交换机上配置，不能有其他交换机上VLAN的成员端口。私用VLAN也能带所有其他类型的Cisco交换机不知道的TLV。 （2）创建主（primary）私用VLAN COS交换机 set vlan primary_number pvlan-type primary IOS交换机 （global） vlan primary_number （vlan-config） private-vlan primary 你必须首先创建主（primary）私用VLAN。后面的步骤要用主VLAN号（primary_number）来绑定次（secondary）VLAN和映射混杂（promiscuous）端口。 （3）创建isolated（被隔离）VLAN和community（群体）VLAN COS交换机 set vlan secondary_number pvlan-type [isolated | community |twoway-community] IOS交换机 （global） vlan

secondary_number （vlan-config） private-vlan [isolated | community] 配置isolated（被隔离）或community（群体）次VLAN来划分端口和控制流量。每一个这样的VLAN的（primary_number）都必须彼此不同和唯一，和主VLAN的number也要不同。Isolated（被隔离）VLAN的成员只能和在第6步中映射的混杂（promiscuous）端口进行通信。双向（two-way）的群体就像一个普通的群体一样，但是有更多功能：能用访问控制列表检查进出（双向）VLAN的流量，而且在私用VLAN内提供了更强的安全性。 （4）把isolated（被隔离）VLAN和community（群体）VLAN绑定到主VLAN上 COS交换机 set pvlan primary_number secondary_number IOS交换机 （global） vlan primary_number （vlan-config） private-vlan association secondary_number_list [addsecondary_number_list] 这条命令把次VLAN关联或者说绑定到主VLAN上。对于IOS命令来说，add选项允许以后关联其他VLAN。 （5）将端口加入isolated（被隔离）VLAN和community（群体）VLAN COS交换机 set pvlan primary_number secondary_number mod/port [sc0] IOS交换机 （global） interface type mod/port （interface） switchport （interface） switchport mode private-vlan host （interface） switchport mode private-vlan host-association primary_number secondary_number 在已经创建和关联好了主次VLAN之后，必须把端口划给VLAN。对于COS交换机来说，可以把sc0接口加到私用VLAN中。 （6）给isolated（被隔离）VLAN和community（群体）VLAN映射混杂（promiscuous）端口 COS交换机 set pvlan mapping primary_number

secondary_number mod/port IOS交换机 （global） interface type mod/port （interface） switchport （interface） switchport mode private-vlan promiscuous （interface） switchport mode private-vlan mapping primary_number secondary_number 在把端口划给次VLAN之后，为了能访问到isolated（被隔离）VLAN或者community（群体）VLAN之外，必须将VLAN映射到一个混杂（promiscuous）端口。 （7）给isolated（被隔离）VLAN和community（群体）VLAN映射MSFC接口（可选） COS交换机 COS set pvlan mapping primary_number secondary_number 15/1 session 15 （privileged）config t （global）interface vlan primary_number （interface）ip address address mask IOS交换机 （global） interface primary_number （interface） ip address address mask （interface） private-vlan mapping primary_number secondary_number 如果您的交换机有一块MSFC，那么可以将私用VLAN映射到MSFC。对于运行COS的交换机来说，要把VLAN映射到端口15/1（对于在于2槽的MSFC来说是16/1），然后将VLAN接口上的IP地址配置为主VLAN的number。对于IOS交换机来说，要找到primary_number的VLAN接口，然后把主次VLAN是映射到那个端口。 提示：你可以配置私用边缘VLAN。3500XL交换机使用受保护端口（protected port）的概念来控制交换机上的流量。3500XL上受保护端口不会向同一交换机上的另一个受保护端口转发流量。这样做和isolated（被隔离）VLAN类似，因为受保护的端口彼此不能通信。使用下面的命令配置受保护的端口。要配置一个私用边缘VLAN，可以选定接口，键入命令port protected。为了核实该端口已经处于受保护的模

式，可以使用命令show port protected。 （8）核实PVLAN的运行 在配置私用VLAN之后，可以使用下面的命令来核实它的运行： COS交换机 show pvlan number show pvlan mapping show pvlan capability mod/port IOS交换机 show vlan private-vlan [type] show interface private-vlan mapping show interface type mod/port switchport 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com