通过巧妙设置确保局域网安全思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E9_80_9A_E8_BF_87_E5_B7_A7_E5_c101_644622.htm 一个企业网的防病毒体系是建立在每个局域网的防病毒系统上的，应该根据每个局域网的防病毒要求，建立局域网防病毒控制系统，分别设置有针对性的防病毒策略。计算机病毒形式及传播途径日趋多样化，因此，大型企业网络系统的防病毒工作已不再像单台计算机病毒的检测及清除那样简单，而需要建立多层次的、立体的病毒防护体系，而且要具备完善的管理系统来设置和维护对病毒的防护策略。 如何设置才能确保内网安全呢，通常可以从一下四个方面进行设置： 划分VLAN防止网络侦听 运用VLAN（虚拟局域网）技术，将以太网通信变为点到点通信，防止大部分基于网络侦听的入侵。 目前的VLAN技术主要有三种：基于交换机端口的VLAN、基于节点MAC地址的VLAN和基于应用协议的VLAN。基于端口的VLAN虽然稍欠灵活，但却比较成熟，在实际应用中效果显着，广受欢迎。基于MAC地址的VLAN为移动计算提供了可能性，但同时也潜藏着遭受MAC欺诈攻击的隐患。 在集中式网络环境下，我们通常将中心的所有主机系统集中到一个VLAN里，在这个VLAN里不允许有任何用户节点，从而较好地保护敏感的主机资源。在分布式网络环境下，我们可以按机构或部门的设置来划分VLAN。各部门内部的所有服务器和用户节点都在各自的VLAN内。VLAN内部的连接采用交换实现，而VLAN与VLAN之间的连接则采用路由实现。目前，大多数的交换机（包括海关内部普遍采用的DEC MultiSwitch 900）都

支持RIP和OSPF这两种国际标准的路由协议。如果有特殊需要，必须使用其他路由协议（如CISCO公司的EIGRP或支持DECnet的IS－IS），也可以用外接的多以太网口路由器来代替交换机，实现VLAN之间的路由功能。当然，这种情况下，路由转发的效率会有所下降。 安全设置局域网文件夹 如今我们所使用的操作系统大多都为Windows XP，可是在安装Windows XP时缺省项的共享都是“ 简单共享 ”，从而导致“ 开放 ”的、不安全的文件共享，我们需要进行如下操作来解除这种不安全的隐患： 首先我们要取消默认的“ 简单共享 ”。打开“ 我的电脑 ”依次单击“ 工具→文件夹选项 ”，在打开的对话框中选择“ 查看 ”选项卡，取消“ 使用简单共享（推荐） ”的选中状态。 然后创建共享用户。单击“ 开始→设置→控制面板 ”，打开“ 用户账户 ”，创建一个又密码的用户，假设用户名为oldforman，需要共享资源的机器必须以该用户共享资源。 接下来设置要共享的目录。假设共享目录为NTFS分区上的目录OLDFORMAN,并设置只有用户oldforman可以共享该目录下的资源。用鼠标右键单击要共享的目录OLDFORMAN，单击“ 共享和安全 ”，点击“ 权限 ”，单击删除按钮将原来该目录任何用户（everyone）都可以共享的权限删除。再单击“ 添加 ”按钮，依次单击“ 高级→立即查找 ”，选择用户oldforman，单击确定添加用户oldforman，并选择用户 oldforman的共享权限。 以后局域网中的计算机要想查看该共享文件夹中的内容，只有输入正确的用户名和密码才能查看或修改共享文件夹中的内容了，如图2。 以交换式集线器代替共享式集线器 对局域网的中心交换机进行网络分段后，以太网侦听的危险仍然存在。这是

因为网络最终用户的接入往往是通过分支集线器而不是中心交换机，而使用最广泛的分支集线器通常是共享式集线器。这样，当用户与主机进行数据通信时，两台机器之间的数据包（称为单播包Unicast Packet）还是会被同一台集线器上的其他用户所侦听。一种很危险的情况是：用户TELNET到一台主机上，由于TELNET程序本身缺乏加密功能，用户所键入的每一个字符（包括用户名、密码等重要信息），都将被明文发送，这就给黑客提供了机会。 因此，应该以交换式集线器代替共享式集线器，使单播包仅在两个节点之间传送，从而防止非法侦听。当然，交换式集线器只能控制单播包而无法控制广播包（Broadcast Packet）和多播包（Multicast Packet）。所幸的是，广播包和多播包内的关键信息，要远远少于单播包。 不管是交换式集线器还是VLAN交换机，都是以交换技术为核心，它们在控制广播、防止黑客上相当有效，但同时也给一些基于广播原理的入侵监控技术和协议分析技术带来了麻烦。因此，如果局域网内存在这样的入侵监控设备或协议分析设备，就必须选用特殊的带有SPAN（Switch Port Analyzer）功能的交换机。这种交换机允许系统管理员将全部或某些交换端口的数据包映射到指定的端口上，提供给接在这一端口上的入侵监控设备或协议分析设备。加强防范观念 安全预防局域网病毒 选择一个功力高深的网络版病毒"杀手"就至关重要了。一般而言，查杀是否彻底，界面是否友好、方便，能否实现远程控制、集中管理是决定一个网络杀毒软件的三大要素。杜绝病毒，主观能动性起到很重要的作用。病毒的蔓延，经常是由于企业内部员工对病毒的传播方式不够了解，病毒传播的渠道有很多种，可通过网络、物理介质

等。查杀病毒，首先要知道病毒到底是什么，它的危害是怎么样的，知道了病毒危害性，提高了安全意识，杜绝毒瘤的战役就已经成功了一半。平时，企业要从加强安全意识着手，对日常工作中隐藏的病毒危害增加警觉性，如安装一种大众认可的网络版杀毒软件，定时更新病毒定义，对来历不明的文件运行前进行查杀，每周查杀一次病毒，减少共享文件夹的数量，文件共享的时候尽量控制权限和增加密码等，都可以很好地防止病毒在网络中的传播。 后记 尽管这些病毒的传播原理很简单，但这块决非仅仅是技术问题，还应该教育用户和企业，让它们采取适当的措施。例如，如果所有的Windows用户都关闭了VB脚本功能，像库尔尼科娃这样的病毒就不可能传播。只要用户随时小心警惕，不要打开值得怀疑的邮件，就可把病毒拒绝在外。 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