不出四步巧妙设置确保局域网安全 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/142/2021_2022__E4_B8_8D_E5_87_BA_E5_9B_9B_E6_c101_142611.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著，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，如图1。图1 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。 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