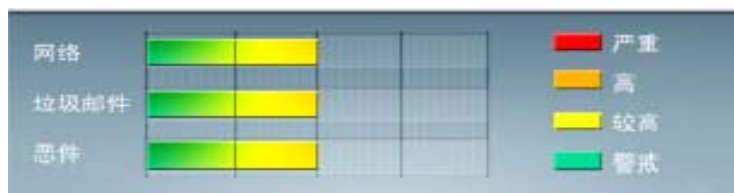


安全威胁每周警讯

2011/03/12~2011/03/19

本周威胁指数



TrendMicro 中国区网络安全监控中心



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	TROJ_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
2	WORM_DOWNAD.AD	蠕虫	★★★★★	→	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
3	WORM_DOWNAD	蠕虫	★★★★★	↑	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
4	TROJ_IFRAME.CP	木马	★★★	↓	GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。当这些文件被执行时，会重定向到这些 URL，并下载恶意程序
5	WORM_ECODE.E-CN	蠕虫	★★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
6	HTML_IFRAME.AZ	网页病毒	★★	↑	网页病毒,通常在网页在插入一个恶意 iframe,用户在访问该网页时会下载恶意文件或重定向到恶意网站
7	WORM_VB.DVP	蠕虫	★★★★★	↑	蠕虫病毒，通过其他恶意程序下载感染或访问恶意网站感染。该病毒会释放 Autorun.inf 到各个驱动盘，在用户访问磁盘的时候以激活该病毒
8	JS_ISTBAR.CN	脚本病毒	★★	↑	Java 脚本类病毒
9	ACM_AGENT.AVGL	脚本病毒	★★	↑	AutoCad 脚本病毒
10	WORM_AUTORUN.CLX	蠕虫	★★	↑	蠕虫病毒，通过网络共享、IRC、P2P、邮件等方式传播。感染该病毒后会在系统自启动项中加入病毒启动信息



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING



系统漏洞信息

MS11-003:Internet Explorer 的累积性安全更新 (2482017)

受影响的软件:

Windows 2003

Windows Xp

Windows Vista

Windows 2008

Windows 7

描述: 请见<http://www.microsoft.com/china/technet/security/bulletin/MS11-003.msp>



系统安全技巧

摘要: 怎样才能有一个令人满意的局域网网速呢? 其实我们只要找出导致局域网网速慢的原因所在, 并进行一些修改与设置, 局域网的网速一定会实现大提速。

怎样才能有一个令人满意的局域网网速呢? 相信每一个企业都无时无刻的与局域网打着交道, 快速稳定的局域网访问速度可以提高办公效率, 这是每个企业的要求。但很多时候并不能如愿, 有时局域网不能访问或者速度极慢。其实我们只要找出导致局域网网速慢的原因所在, 并进行一些修改与设置, 局域网的网速一定会实现大提速。

揪出局域网网速慢的背后黑手

断网的故障排除起来可能容易一些, 但网络是通的, 速度变慢解决起来可能要麻烦一些。造成局域网网速变慢的原因主要有以下几点:

广播风暴导致网速变慢。处于同一个网络的所有设备位于同一个广播域, 而所有的广播信息都会播发到网络的每一个端口, 同一时间只能有一个广播信息在网络中传送。网络中的计算机数量不断增多, 广播包的数量也会急剧增加, 广播所占用的时间也会越来越多, 当广播包多到一定程度就会对网络上的正常信息传递产生影响, 造成网络的传输效率明显下降, 甚至会造成网络瘫痪。另外, 一些流行的网络病毒及黑客软件的攻击也会造成广播风暴。

网络设备及器材故障引发网速变慢。如果计算机的网卡或其他网络设备发生物理损坏, 损坏的网卡会不停的向交换机发送大量数据包, 这其中有很多数据包是无效的, 大量无用的数据包会造成信息传输延时, 引起网络堵塞, 从而导致广播风暴, 造成局域网网速变慢。这可以采用替换法来排除网络设备的故障, 其中网卡、集线器以及交换机是最容易出现故障的设备。

需要注意的是, 网线也可以导致速度变慢。很多公司在组网的时候, 没有刻意考虑网线的质量, 认为好坏无所谓, 速度上没什么差别。但是在 100M 的网络中, 杂牌网线和一些名牌网线会有明显不同的传输速度。水晶头的制作也是有讲究的, 很多朋友认为只要线两端水晶头的次序一样就行了, 这种认识也是错误的。双绞线是由 4 对线紧密而合理地缠绕在一起的。按照 T568A、T568B 标准制作的水晶头, 可以最大限度的避免串扰, 保证数据快速稳定传



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING

输。如果不按照这个标准制作，可能开始使用的时候正常，过一段时间网速就会变慢。

网络回路导致网速变慢。在连接比较复杂的局域网网络中，有的网管可能使用备用线路，一时马虎却将备用线路当成了主线路连接，这样在无意间造成了网络回路。在网络回路里，数据包会不断发送和校验数据，这会严重影响整体的网络速度。在组网的时候，在网线上贴上标签可以减少这种故障的发生，同时贴标签对排除网络故障也有帮助。这类故障可以采用分区分段逐步排除的方法找出问题所在。

病毒影响导致网速变慢。如今，病毒对网络的负面影响不可低估。由于防卫不当，局域网内部有的计算机机会感染病毒，一些蠕虫病毒会不断的对局域网内的其他计算机发送病毒，还有一些病毒可以随机选择电脑中的文档附加在通讯簿上的邮件地址发送，成千上万的垃圾邮件排队往外发送，有的邮件被阻止后又成堆地退回来堆在服务器上，造成网络明显拥塞，速度急剧变慢。这可以通过打补丁、关闭端口、及时升级杀毒软件等措施来加强网络安全。

此外，网络中有些设备的端口瓶颈也可以造成网速变慢，这可以通过安装多个网卡、划分多个 VLAN、改变路由器配置来增加网络带宽，有效地缓解网络瓶颈，提高数据传输速度。如果你的企业使用的是无线局域网，那么无线路由器的位置摆放不当，会造成信号微弱，从而影响局域网网速变慢。

局域网加速绝招

找出导致局域网网速变慢的故障之后，我们就可以对症下药了。前文已经简要介绍了故障排除的基本方法，用这些方法排除故障之后可以加速局域网的网络速度。此外，还有一些技巧可以加快局域网网速。

让网卡全速工作。右键单击“我的电脑”图标，依次打开“属性→硬件→设备管理器”选项，然后单击“网络适配器”选项，选择相应的网卡，双击后在打开窗口中单击“高级”标签，选中“LinkSpeed/DuplexMode”（连接速度/双工模式）这一项，默认情况下是“Automode（自动模式）”，在下拉列表框中选择“100FullMode”（全功模式）即可，这样可以吧网卡调至全速。

断开不用的网络驱动器。使用映射网络驱动器可以加快局域网的文件夹访问速度，可是如果你映射了网络驱动器后，以后不在使用了，一定要将其断开，因为每次开机时系统会自动映射此盘，占用较多的系统资源，从而让局域网访问速度变慢。断开的方法是：

打开“资源管理器”，单击“工具”→“断开网络驱动器”命令，然后在打开的窗口中取消相应的驱动器即可。也可以在桌面上右键单击“我的电脑”图标，选择其中的“断开网络驱动器”即可。

直接访问加速访问网上邻居。如果你知道局域网中需要访问的计算机名称或固定IP地址，你可以在“资源管理器”的地址栏中直接输入你需要访问的共享文件夹所在的计算机或者该网络路径则可以快速访问。比如如输入“[\\Server\公司制度](#)”就可以快速进入名称为“Server”计算机中的“公司制度”共享文件夹，查看其中的内容。另外，你也可以打开“开始→运行”，在窗口中输入“[\\192.168.0.11\公司制度](#)”来快速访问共享文件夹，其中的“192.168.0.11”为局域网中的共享文件夹所在电脑的固定IP地址，而通过“网上邻居”一层一层地打开。

关闭无关的选项。在 WindowsXP 操作系统中，打开“控制面板”中的“文件夹选项”，单击“查看”标签，在“高级设置”窗口的最下方有一个“自动搜索网络文件夹和打印机”选项，默认状态下是选中的，但你可以把它关闭。因为这个选项让系统在开机时会自动搜寻网络文件夹和打印机，使启动速度变慢，而且这个选项还可能让你的机密文件被打印到其他部分的打印机上去。关闭以后，打印时可以在打印选项中选择网络打印机即可。这样通过“网上邻居”来访问局域网的电脑时，系统将不会自动查找共享文件夹，这样也提高了局域网访问速度。

无线局域网加速绝招

如果你的公司采用的是无线局域网，可以通过下列方法来提高局域网的网速：

排除干扰，移除遮挡物。无线设备之间如果存在遮挡物，尤其是一些金属遮挡物，这将严重影响无线信号的传输，所以一定要移除这些遮挡物，可以将无线 AP/路由器置于房间内较高的位置，最好放在房间的中间，这样可以公司的所有网卡都能更好的连接上。另外，公司中的无绳电话、微波炉等电器设备对无线传输信号有很大的干扰。有的微波炉使用 2.4GHz 频段上第 7 到第 11 个 Channel，对于采用 IEEE802.11b 协议的无线设备，可以把通讯频道设置为其他范围即可。当然也可以让这些电器设备远离无线设备，给他们搬个家。

小提示：还可以使用增益天线来提升区域的信号辐射强度，但一定要选择名牌大厂的产品，某些杂牌产品起不到真正的作用，形同虚设。

此外，还可以打开 54Mbps 模式。部分无线 AP/路由器为了“兼容”更多的无线网卡，并没有打开它的 G 模式，我们可以将“无线模式”设置为 Gmode（G 模式），将“传输(TX)率”设置为 54Mbps，激活 8X 模式，并将“天线传输功率”设置到最高，以此来加速无线网络的传输速度。无线 AP/路由器的一般登录地址为 <http://192.168.0.1> 或 <http://192.168.1.1>。

小提示：打开 54Mbps 模式后，有的 PCMCIA 插槽的无线网卡上可能连不上无线 AP/路由器，这时改回 mixedmode（混合模式）即可。

最后，还要查看是否开启了无线网卡的节能模式，如果开启，请关闭此功能，因为在节能模式下，无线网卡的发射功率会有下降，导致无线信号的减弱。最好使用无线设备自带的管理程序来管理设备，这样可是设置更多的选项，而 WindowsXP 的无线管理显得有些“单薄”。

通过上面介绍的这几种方法，相信你的局域网速度会有很大的提升。当然，提高局域网网速还有其他的方法，这需要在实践中不断摸索总结。

来源：eNet

免责声明

该邮件列表仅用于提供信息，此邮件列表内容不负任何担保责任，没有明示或默示的保证，包括但不限于对适销性、特定用途适用性以及不受侵害的暗示保证。用户对此邮件列表的准确性和使用承担全部风险，因依赖该资料所致的任何损失，趋势科技均不负责。



ANTI-SPYWARE



ANTI-SPAM



WEB REPUTATION



ANTIVIRUS



ANTI-PHISHING



WEB FILTERING