网络安全

安全技巧（十三）

小未 主编

目录

交换机如何工作

交换技术是一个具有简化、低价、高性能和高端口密集特点的交换产品，体现了桥接技术的复杂交换技术在 OSI 参考模型的第二层操作。与桥接器不同的是交换机转发延迟很小，操作接近单局域网性能，远远超过了普通桥接互联网之间的转发性能。

交换技术允许共享型和专用性大的局域网段进行带宽调整，以减轻局域网之间信息流通出现的瓶颈问题。现在已经有以太网、快速以太网、FDDI 和 ATM 技术个交换产品。

三种交换技术

1。端口交换

端口交换技术最早出现在插槽式的集线器中，这类集线器的背板通常划分有多条以太网段，不用网桥或路由器连接，网络之间是互不相通的。以太主模块插入后通常被分配到某个背板的网段上，端口交换用于将以太模块的端口在背板凳多个网段之间进行分配、平衡。根据支持的程度，端口进行还可以细分为：

*模块交换：将整个模块进行网段迁移

*端口组交换：通常模块上的端口被划分为若干组，每组端口允许进行网段迁移。

*端口级交换 :支持每个端口在不同网段之间进行迁移。这种交换技术是基于 OSI 第一层上完成的，具有灵活性和负载平衡的能力等优点.如果配置得当,那么还可以在一定程度进行容错,但没有改变共享传输介质的特

点,因而不能称之为真正的交换.

2.帧交换

帧交换是目前应用最广泛的局域网交换技术,它通过对传统传输媒介进行微分段,提供并行传送的机制,以减小冲突域,获得高的带宽.一般来说每个公司的产品德实现技术均回游差异,但对网络帧的处理方式有一下几种:

*真通交换:提供线速处理能力,交换机只读出网络帧的前 14 个字节,便将网络帧转送到相应得断口上.

*贮存转发:通过对网络帧的读取进行验错和控制.

前一种方法的交换速度非常快,但缺乏对网络帧进行更高级的控制,缺乏智能性和安全性,同时也无法支持具有不同速率的端口的交换.因此,各厂商把后一种技术作为重点.

3.信元交换

ATM 技术代表了网络和通信中众多难题的一剂"良药".ATM 采用固定长度 53 个字节的信元交换.由于长度固定,因而便于用硬件实现.ATM 采用专用的非差别连接,并行运行,可以通过一个交换机同时建立多个节点,但不会影响每个节点之间的通信能力.ATM 还容许在源节点和目标节点之间的通信能力.ATM 采用了统计时分电路进行复用,因而能大大提高通道德利用率.ATM 的带宽可以达到 25M、155M、622M 甚至数 GB 的转送能力。

局域网交换机的种类及选择

局域网交换机根据使用的网络技术可以分为：

*以太网交换机

*令牌环交换机

*FDDI 交换机

*ATM 交换机

*快速以太网交换机交换机

如果按交换机应用领域来划分，可分为：

*台式交换机

*工作组交换机

*主干交换机

*企业级交换机

*分段交换机

*端口交换机

*网络交换机

局域网计算机是组成网络系统的核心设备。对用户而言，局域网交换机最主要的指标是端口的配置、数据、数据交换能力、包交换速度等因素。因此，在选择交换机时要注意一下事项：

1.交换端口的数量

2.交换端口的型号

3.系统的扩充能力

4.主干线的连接手段

5.交换机总交换能力

6.是否需要路由选择能力

7.是否需要热切换能力

8.是否需要容错能力

9.能否与现有设备兼容,顺利衔接

10.网络管理能力

边界路由概念

边界路由系统体系结构是一种令广域网(WAN)设计人员极感兴趣的创新软件技术，这种技术可以极大地简化 WAN 外围的全功能路由。因此，它第一会使降低很昂贵的 WAN 维护费用成为现实。除边界路由的软件优势外，边界路由还可在不限制所支持的协议的前提下，节省访问与路由有关的远程硬件费用。

所谓边界路由是将标准的路由软件看作 n 路本地路由，并将软件中的局域网部分扩展到广域网。这将导致远程路由器采用一套全新的、并且是极大简化了路由软件功能。

换言之，边界路由把中心和远程的设备看作一个单一系统，而解决路由问题的这一创新提供了只配置单个接口的所有优点，该接口极类似于在一个集中式主干网 LAN 环境中的中心设备，不过在大型 WAN 网络中。由于很少需要配置中心或远程路由器的 WAN 端口，从而减少了管理的复杂性。

边界路由的软件创新为与访问路由器有关的硬件优势又增加了简单和廉价等优点，但它并不限制在远程点对路由协议的选择。

边界路由通过把路由管理的复杂性转移到一个路由管理中心来简化对路由器的管理；有了边界路由，网络管理员能够迅速而有效地管理多个远程地点。如果 WAN 连接需要从边界路由转移到通常的路由，那么软件升级工具便可以快速地把一台远程边界路由设备转换为一

台通常的路由器。边界路由支持以下强大的路由改进能力：

数据压缩，它允许在低速线路上运载更大的信息流量，并极大地降低 WAN 成本。

服务类，实现数据优先化以便加速关键应用的处理。

可灵活设置的过滤，以提供网络安全和流量控制。

交换式线路支持，包括支持帧中继、ISDN、拨号线路以及 X.25，以降低远程办公室 WAN 连接的成本。

故障恢复能力，当路由器检测到主线路故障时，可提供拨号备份。

基于对整个系统的代理识别而进行功能强大的网络管理。

边界路由技术通过将大多数路由器操作集中起来，使中央办公室的几个全功能路由器，能够为网络外围的低成本路由器提供服务的方法来降低购买设备的费用。

防御来自网络的攻击

从没有如此的尴尬，面对攻击，竟然束手无策，你用尽了全力，却还是枉然，你思考着这一切的发生，终于明白在这数字化空间里，有喜悦，有悲伤，更还有那许多熟悉的陌生人给你的网络攻击，有的可能是善意的，一个玩笑，但更多的是伤害，威胁，当然，攻击不是网络的全部，但它是对网络最大的亵渎，破坏了网络赖以维系的准则，即使在今天，你还平安而惬意的冲浪在网海里，可能你并不以为网络攻击的威力会有多大，但我想对你说，在网络上，数字化方式的保存是非常容易的，

但它的失去更容易，一次的意外，将使得你永远失去，这就是网络，那不确定的精灵。虽然你我不能够抵御完全的网络攻击，但可以把它减少到最低，削减它的能量，其实，有些攻击都是自己的疏忽造成的，不管怎样，请跟随我去看看那来自网络的攻击……

一、第一步，该怎么做

第一步要从保护自己的名字开始，在网络里每一个人都会有一个 ID，即用户名，你可以起一个与真实名不同的名字，你知道，在现实生活中，别人往往都是通过名字来识别你的，同样，在网络里，别人也是通过 ID 来识别你，不管出于什么目的，你可能不愿意别人从你网络上的 ID 名来识别出你现实中的身份，所以，在起名时一定要记住，不要用一些太过招摇的名字，虽然，你可以这么做，但你往往比那些“平凡”人冒更多风险，因为有时候，网络的攻击是随意的。(我再次要强调，网络不是到处充满着危险，步步为营，而只是我现在要谈它。)

还有，当你在 ISP 注册用户名时，你起的 ID 名将和你电子函件地址相关联，此时，起名不要用太过简单的名字，一般 ISP 允许八个字母，所以，尽量全部用到，或者至少用到五个字母，如果你起个名字是 love,那么，别人很容易就记住了你的电子函件地址，而如果你在 love 后面加上几个数字，比如 love3282,我想就没那么容易记得吧，可能你会觉得这样破坏了自己的形象，其实在网络里，电子函件地址好像只是一个房间的门牌号，而房间中的你可以塑造另外的许多名字。

大家都知道，网络里女性朋友是很少的(现在逐渐增多)，而她们最能够引起大家的注意，不管在网络的哪里，

girl 都是最受欢迎的，而此时，这些女性用户往往要承受更多的压力及攻击，所以，起名对于女性用户更是重要，其实，作为平等，女性朋友也应该起符合自己身份的 ID，我不反对这点，但作为女性的你，想到没有，名字的暴露，使得你每天收到大量的来信，而其中掺杂着些许的骚扰，此时你该如何呢，这就是网络，它不同于现实生活，在这里，你会受到更多的注意。当你起名时，请一定要慎重。但有另外一种情况，冒名的，就是男性起一个女性化的名字，说着女性化的言语，善意的，会在某一段对话结束后揭穿他的身份，而恶意的，会欺骗你，让你沉迷网络里的幻想。

总的来说，对于网络起名，我们要分清不同的场合，有时需要真实，有的需要匿名。而此时，你要牢记，有人在注意着你，他在网络的那一头。

二、谁控制信息

1.电子函件

电子函件的规则是很简单的，当在“写”电子函件的时，你能控制自己该如何表达，别人才会明白，并且觉得亲切,这些你当然有一套,但当你单击了 Send 按钮后，这些信息发出去了吗，当然，但你想过没有，这些信息在转送过程中，会受到阻碍吗，我并不是说中转的那些服务器，而是指陌生的攻击者，可能你会认为，网络这么大，怎么会有人对我的信，感兴趣，的确，你说的很对，我一直都这样认为，我作个假设，你写了一封情书，然后发送了出去，可是想到要是被人截住了怎么办，你并没有写那些露骨的言语，但那种被公开的感觉实在不好受，但值得你庆幸的是，截住电子邮件并不那么容易，大家都知道，网络在传输信息时，会把该信息分解成许

多的小包，然后再通过不同路径传输，这样，有人如果真的想截你的信息，除非它在源头截住，那将是非常困难的，因为源头的那个人，就是收信的人，但不表示没有可能，其实，这只是个心理问题，毕竟你我没有秘密。

还有一个人能看到你的信，这就是 ISP 的管理员，网络是需要控制的，信息也一样，而管理员就是控制信息的人，当然，我要说，目前还没有这么无聊的管理员，但他(或者是她)的确能看到你的信息，怎么办，加密吗，没有必要，其实，你有权利知道谁还能控制你的信息，知道后，就会有准备了。以下是一些好的提议：

1)不要利用免费的 SMTP 服务器发信；

2)对于重要的信，要让收件人回复确认；

3)慎重公布你在 ISP 的电子函件地址；

4)对于秘密信息，最好通过其他渠道传送，如果实在需要利用网络，请加密信息;

5)仔细检查收信人的电子函件地址，一点错误，别人就收不到了。

2.口令

这是目前谈的最多的话题，而我还要再谈。

口令曾经令人很有成就感，因为只有你能进一些别人进入不了的地方，那种感觉实在美妙，可惜，事过境迁，现在口令太多，在网上很容易就可以获得口令，我，已经拥有无数口令，但已经没有那种成就感了，剩下的只是麻木，输用户名，输口令… …但此时，你要清醒了，有些口令是很重要的，失去对它的控制，将使得你损失一些什么东西，金钱或者是麻烦。

什么口令最重要呢，当然是你注册 ISP 时的口令，

因为他(或者是她)是你进入网络之门的钥匙，如果你的钥匙太简单，别人很容易就会复制一份，现在有种最原始的黑客软件，它有一个数据库，其中列出了无数的组合，利用它就可以猜用户的口令，一个个的试，比如你起了个口令是 123456(没有人会这样吧)，那么，这是黑客软件最基本的组合，没有一秒钟，口令就被破解了。以下是些好的建议：

1)在你第一次上网时，记得马上更换口令，这时是最容易被破解的；

2)不要用你很容易就记住的口令组合，比如你生日或着你爱狗的名字；

3)要经常更新密码，最少两个月更新一次；

4)慎重选择让软件自动记住口令功能，特别是与其他人共用计算机时；

5)在你没有求助 ISP 时，ISP 不会主动询问你的口令，记住；

6)如果必须要把口令泄漏给某人，一定要在别人使用完后，马上更换；

7)把口令写在纸上，但请记住让它远离电脑。

怎样判断自己的口令被破解呢：

1)登录 ISP 时，总是提示错，让你再次输入口令；

2)当你在 ISP 查阅上网时间时，发现你没有上网时，而“你”却在上网；

3)收到许多陌生人的来信；

4)发现有人在 BBS 里以你的名义发布信息，但这 BBS 是需要口令的；

5)每个月去缴付上网费用时，发现与你的习惯不符时。

现在一些破解别人口令的人，很聪明，他都不更换别人的口令，而且也只会在你不会上网的时间里上网，让你无从察觉，所以，你一定要随时注意你帐号的使用情况，好啦，如果发现口令被盗，要采取什么办法呢：

1)马上更换口令，如果能改的话，并且尽快通知 ISP；

2)复制你上网的时间表，并标明在这张时间表上某段时间内你没有上网；

3)马上发布声明，表示你对某些发表的言论并不负责任；

4)向当地公安机关报案。

总之，最有效果的办法，就是让别人不能取得你的口令。

三、Web 的内幕

Web 是网络里最迷人的景色，它使得无数的冲浪好手神往，绚丽多姿的页面，丰富超前的信息，使得许多人流连忘返，但你是否知道，当你惬意地浏览信息时，Web 对你做了些什么呢，当然它不能窃取你身上的钞票，而只是给你的“未来”带来麻烦。

1)提交信息

现在有许多 Web 页会让你提交某些关于你的信息，比如姓名，性别，地址等等，你可能在填写时，并不会提供这些信息，你是对的，因为它可能会恶意地要得到你的这些信息，但有时候，网站提供某些免费服务，而你要付出的某些代价就是提供个人信息，那么这时，你可以填写，但别填真的，这并不是欺骗，因为该网站并没有能力让你相信它，这是它的失误，如果你相信某人，你会告诉他某些关于你的信息，但你现在并不信任该网

站，所以，就告诉它假的吧，特别是对上网的儿童，家长一定要教育它，不要提供任何关于他或者是家的信息给任何地址，即使某个地方说它很安全。在这里，我并没有偏激到说任何地方都不可信任,只是在作出选择时，要慎重。

2)Cookies

Cookies 是网站收集浏览者信息的工具，它真正在幕后工作，在你没有察觉时，它在你的系统里写下某些信息，当然有些是善意的，只是为了给你提供更方便的浏览组合，但有些 Cookies 是恶意的，它窃取你某些个人信息，在你系统里写下某些恶意的记录，其实，这些倒不是很可怕，因为你可能不会再次浏览某站点，但这不代表你可以轻视它，现在的浏览器都禁止接受 Cookies 的写入，笔者觉得这是个好办法，虽然有时会损失某些网站提供的服务。

3)Java Script

Java Script 在网页的流行产生了一些安全问题，一些安全被堵住，另一些又产生了，恶意的网站建设者，会利用 Java Script 把一些破坏程序转移到你的系统里，然后大肆破坏，所以，你可以在觉得危险时，关闭接受 JavaScript 功能,还要注意某些浏览器的安全升级,这样，把 JavaScript 的危害减到最低。

4)你的踪迹

当你拜访某站点时，你会发现在主页上看到，欢迎你 XXX，第 XX 次来到我的站点，什么，它怎么知道的，你告诉它的吗，没有呀，看来你的个人信息泄漏了。

某些网站能知道你是来自哪里、曾经拜访过那些网站、使用计算机的类型、操作系统的类型、什么浏览器，

一个 CGI 程序就能收集到这些所有信息，可怕吗，并不，因为这些对你来说，并不重要，真这样吗，有些网站会收集拜访者的电子函件地址，然后发送轰炸的邮件或者那令人恼火的垃圾信(广告)。我说了这些，不是说，你不能再浏览 Web 页了，只是小心点罢了。

四、交互的危险

网络的魅力在于交互，人与人能自由的交流，彼此诉说心声，但过度的交互有时会给人带来麻烦，网络的操作是很简单的，有时，容不得你后悔，一个单击，某些信息就发送了出去。

所以，当你在提交或者发送某些信息时，一定要慎重。

1)E-Mail

E-Mail 是除了 Web 外第二个最有魅力的工具，它快捷、方便，使得许多人趋之若鹜，而去邮局的机会都大大减少了，E-Mail 也是最容易遭到攻击的地方，因为只要知道你的电子函件地址，任何人都可以给你发送信息，有的是善意的交流，而有的是恶意的攻击，你并不能完全避免它，但可以把它的威力减少到最小。

如果有人通过 E-Mail 骚扰你，你在收到第一次这样的信时，保持沉默，如果再次收到，你可以礼貌的让他停止这样做，但一般不会见效，对于那种比较初级的骚扰者，你可以通过他的电子函件地址找到他来自哪里，首先你写一封信给他邮件地址的 ISP，让他们帮助你查找或者停止该帐号的使用，如果骚扰者的电子函件地址并不能够使得你知道他来自哪里，你也可以利用邮件程序查看全部信息，包括信件头，在这里，列出了该信件的来自哪里，经过了哪些服务器，等等，虽然你还是不

知道他是谁，但至少你找到了他的踪迹。如果骚扰升级怎么办，难道没有办法了吗？此时，你要求助自己的 ISP，因为他们会有自己的技术及方法，侦察该骚扰信的发源地。

对于电子函件地址，还要注意，不要打开任何陌生的附件，特别是一个执行文件时，除非你能确定它是什么，否则即刻 DEL，因为许多病毒都是通过这样的方式传播的。

2)BBS 问题

BBS，电子公告牌系统，是一个迷人的地方，许多人在这里交流，述说自己的故事，而有时，这里有些不和谐的音符，使得你不得不重新审视这片空间。

目前，许多 BBS 需要注册，每次进入都需要口令，这对防止滥用 BBS 起到阻止作用，但可惜的是，只要你拥有一个任何的免费邮件地址，都可以去注册一个 ID，这样，心怀叵测的人总会利用某些漏洞来进行他不可告人的诡计，那么，这些人会给你什么攻击呢，首先，这些人在 BBS 上出现，是非常道貌岸然的，让人觉得他非常可爱，然后，他会主动与你联系，与你建立友谊，等你信任他后，他会提出某些要求，比如让你提供某些信息给他，比如住址，电话等等，虽然，我猜不到，他们要这些信息有什么用，但他们就是这么问的，其实，对于我们这些老网民来说，我们会分辨这些状况，但对于初上网及儿童用户来说，有时候，他们受不住某些诱惑，而就范。当然，BBS 不是这么可怕，但我说的这种人，无时无刻不在，你注意了吗……

3)下载，美丽的诱惑

网络是个宝藏，让你永远也挖掘不完，而此时，面

对美丽的诱惑，你要清醒，因为在它背后，可能有不可告人的黑幕，目前广为流行的 CIH 病毒，就是通过下载软件传播的。而有的网站，让你下载某个程序，说通过它可以看一些隐秘的图片，而一些涉世不深的网民，下载该软件后，等待你的将是什么呢，该软件切断了你与 ISP 的连接，而偷偷把你的电话拨到某个小国，的确你也看到了你想看的东西，但等到你缴付费用的那天，你会明白了一切，网络充满了诱惑，你需要以下的提示：

? 下载时要小心，看清楚该软件的说明，大小，下载地点，如果该软件没有任何的说明，请不要下载；

? 如果对于怀疑的软件你还想用，那请对重要数据备份；

? 如果你在网页上到处看到 FREE(免费的意思)，请注意，这往往是个骗局，不要触摸网页上的任何东西；

? 下载软件后，要用病毒软件检查，看软件是否含毒；

? 在使用下载软件时，一定要查看 readme 文件，如果该软件只有一个执行文件，请慎用，除非你知道它是什么。

4)网络爱情

网络有爱情，我相信，但网络也有它特殊的一面，你要看得清楚。

网络容易让人产生错觉，距离产生美，网络给了你幻想的空间，此时，你很容易堕入情网，虽然多数是你一厢情愿的，而某些居心叵测的人，会利用装扮女性网友(或者本身就是女性)来欺骗某些善良的求偶者。

上网寻找爱情，对于那些害羞的人来说，的确很容易，方便，在家即可寻觅，而且无需花钱，不必怕自己

某些动作而失态，可以完全掩盖自己的缺陷等等，更重要的是，它很新奇。一般你要多思考一些问题，对方是谁，长的什么样，她的言语的确诱人，但她的人呢，有许多这类约会的人，会有经验，不要轻易逃离网络见面，那是很“可怕”的。

不管怎样，不要轻易告诉你的网络恋人你的电话，住址等，因为这样，以后要摆脱容易得多，不然可就麻烦了。在网络里，感情很容易释放，但要小心你的心，网络里有爱情，也有欺骗。

六、Internet 神话

网络里充满了神话，一夜致富的商业机会在网络里到处荡漾，一不小心就遇到了它，网络的确能给人机会，但那不像有些人说的，是那样的容易。

现实中的欺骗在网络里出现了,你见不到那个人,而只会收到一封充满众多诱惑的信,什么可以通过某些方法赚多少美元,前提条件是,要给那个人寄去多少钱;可能那个人,给你发了一封信,并附带上五个人的邮件地址,它让你给第一个人寄去 1 美元,然后把它去掉,并且把自己的邮件地址排在后面,然后发送出去,任何人都行,越多越好。如果正常,你就会在未来的日子里收到一张张汇款单,很伟大的发财方法,可惜这一切不会正常的发生,即使它没有带给你现在的麻烦(还是有),但带给你的是未来的麻烦,能承受吗,其实,这一切,发生的概率很小,因为我们很聪明,从来没有对它感兴趣过,更重要的,这些骗人的把戏,都是飘洋过海来的,在那全是英文的信中,可能我们只会对那大大的美元符号$记忆犹新.

如何发现欺骗呢，以下是一些提示：

1)收到一封信，说什么这是个伟大的机会，让你致