论计算机网络的安全性设计

摘要

在计算机与网络技术飞速发展的今天，医院信息系统的建设已经成为医院现代化管理的重要标志，同时也是医院管理水平的一种体现。尤其是医疗保险制度的改革，与医院信息系统形成了相互促进的态势，我国很多医院都建立了自己的信息系统。由于行业性质的缘故，医院信息系统必须 7 X 24 小时不间断运转，因此对网络系统的安全性和可靠性有很高的要求。本文通过一个医院信息系统项目，阐述了医院计算机网络的安全性设计方面的一些具体措施，并就保障网络的安全性与提高网络服务效率之间的关系，谈了自己的一点体会。

正文

我于 2001 年 4 月至 2003 年 10 月参加了某医院的医院信息系统的建设工作，在项目中，我担任了系统分析与系统设计工作。医院信息系统是指利用计算机软硬件技术、网络通讯技术等现代化手段，对医院及其所属各部门对人流、物流、财流进行综合管理，对在医疗活动各阶段中产生的数据进行采集、存贮、处理、提取、传输、汇总、加工生成各种信息，从而为医院的整体运行提供全面的、自动化的管理及各种服务的信息系统。由于行业性质的缘故，医院信息系统必须 7 X 24 小时不间断运转，因此对网络系统的安全性和可靠性有很高的要求，在该项目的系统设计阶段，我们就将网络系统的安全性作为一个重要部分考虑在内。由于该信息系统是建立在一个物理上与公众网完全隔离的局域网基础上的，所以我们并没有过多地考虑防御来自外部入侵者的威胁方面的安全问题，我们认为该系统的安全核心一是保证信息系统的正常运行，二是保证数据的安全，也就是说该医院网络信息系统的安全可以分为信息系统安全和数据安全。下面就我们在这两方面所采取的措施加以论述。

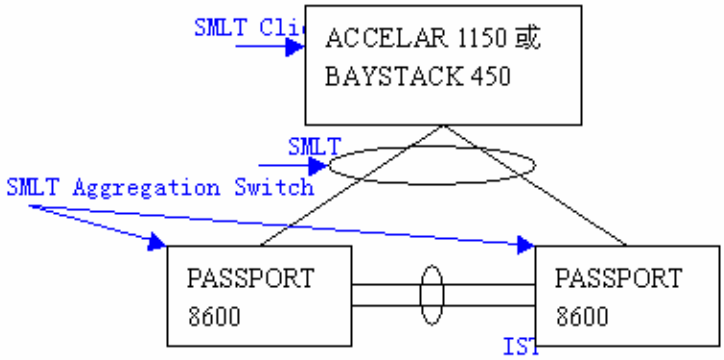
信息系统安全

信息系统安全涉及网络安全、服务器组的安全、供电安全、病毒防范等。

1、网络安全

对于医院的业务局域网，威胁网络安全的主要因素有：网络设计缺陷、网络设备损坏、非法访问等。经过充分调研，认真分析，结合该医院的的实际情况，我们设计了一个主干为三层路由千兆交换以太网的网络方案。

我们采用具有三层路由功能的两台核心交换机 NORTEL PASSPORT 8600、两台具有三层路由功能的 NORTEL ACCELAR 1150 交换机和千兆级光纤组成网络主干，边沿交换机为 BAYSTACK450。本方案我们采用 SMLT（Split Multi-Link Trunking）+VRRP（Virtual Router Redundancy Protocol）技术。NORTEL 公司的 MLT（Multi-Link Trunking）是一种允许多条物理链路模拟成一条逻辑链路的聚合链路协议，它通过将两个交换机之间（或交换机与服务器之间）的两条或以上的物理传输链路虚拟为一条逻辑上的传输线路进行数据传输，进而可以成倍地提高两个交换机之间（或交换机与服务器之间）的数据传输带宽，同时提供了传输链路的冗余备份。当构成虚拟传输链路的几条物理链路有一条由于端口或传输介质本身失效时，不会影响数据的正常传输，所受到的影响仅仅是虚拟链路的传输带宽。SMLT，分离的多链路聚合主干，同 MLT 相比，SMLT 在构成上，不再是两个交换机之间，SMLT 的一端是一个支持 MLT 的交换机，而另一端则是由两个交换机通过 IST（Inter Switch Trunk，是连接两台聚合交换机以实现信息共享，使两台聚合交换机能作为一台逻辑交换机运转的点对点链路）形成的一个逻辑上的交换机。MLT 交换机分别与这两个 SMLT 交换机连接，因此，SMLT 在增加带宽的同时，可以提供最高级别的可靠性——交换机级别的可靠性。两个 SMLT 交换机不论是端口失效还是端口模板失效，甚至是交换机失效都不会影响数据的正常传输，避免了单点失效对网络正常连通带来的影响。同时，传输负载由两个交换机来均衡完成，可以大幅度提高网络主干的传输性能。SMLT 体系结构由 SMLT Aggregation Switch、IST（Inter Switch Trunk）和 SMLT Client 构成，其结构图如下：



在没有使用 SMLT 的情况下启动虚拟路由冗余协议（VRRP），通常只有主交换机进行数据包的转发，如果主交换机出了故障，备用交换机会自动顶替主交换机，完成数据包的转发工作；使用 SMLT，使得 VRRP 的性能得到扩展，除了主交换机进行数据包的转发外，备用交换机也进行数据包的转发，主交换机和备用交换机互为备份并互相侦听，这样既可以实现流量的负载均衡，也可以实现故障恢复，避免单点失效。为了避免边沿交换机出现单点失效，我们采用了堆叠技术，把若干台 BAYSTACK450 用堆叠电缆堆叠起来，在堆叠的某些交换机上加装光纤模块，由这些光纤端口捆绑成一条逻辑链路上联到网络主干，这样就算堆叠中的某台交换机损坏了，整个堆叠还可以正常工作。特别地，门诊收款处和门诊药房是医院的窗口单位，为了避免由于门诊楼交换机堆叠中的某台交换机出现了故障而导致门诊收款系统和门诊发药系统瘫痪，我们把门诊收款工作站和门诊发药站分散地接到堆叠中的七台交换机中。

在防止非法访问方面，我们采用了密码管理、权限设置、虚拟子网（VLAN）的划分等措施。

2、服务器组的安全

服务器是全院计算机网络的大脑和神经中枢，保证服务器可靠长期有效的运行是网络信息系统安全的一个特别重要的问题。

由于本方案中的应用程序是采用安全性较高的三层体系结构，所以服务器组包括域控制

器、应用服务器和数据库服务器。

域控制器我们采用了两台稳定性较好的 IBM xserials 230 服务器，一台做主域控制器，另一台做备份域控制器，这样既可以实现登陆验证的负载均衡，又可以避免域控制器的单点失效问题。

应用服务器部分我们采用了六台 HP 380G3 服务器和一台 F5 BIG-IP5000 控制器。BIG-IP 控制器是针对企业本地网站或数据中心的一种产品。它能够提供高可用性和智能负载平衡功能。六台 HP 380G3 服务器通过 F5 BIG-IP5000 控制器连接到核心交换机 PASSPORT 8600，F5 BIG-IP5000 控制器可以持续监视六台 HP 380G3 服务器，以确保服务器运行正常，然后再自动将输入的服务请求路由到六台中可用性最高的服务器。这样连接，只要有一台 HP 380G3 服务器不出现故障，中间层应用程序便可以正常运行。这样设计既可以实现中间层应用程序的负载均衡，同时在 F5 BIG-IP5000 控制器不出现故障的前提下，又避免了应用服务器的单点失效问题。

数据库服务器部分我们采用了一台稳定性较高、存储性能较好的 HP DL760 G2 服务器、一台 HP DL580 G2 服务器和一台 HP MSA1000 光纤磁盘阵列柜。两台服务器分别通过光纤通道连接到磁盘阵列柜，组成存储局域网（SAN）。本方案采用了微软的群集技术，实现了 Active/Passive 双机热备份模式，HP DL760 G2 做主数据库服务器，HP DL580 G2 做备份数据库服务器，在主服务器发生故障的情况下，备份服务器将自动在 30 秒内将所有服务接管过来，从而保证了数据库服务器的正常运行。在磁盘阵列柜，我们安装了 5 块 146G 的 SCSI 服务器硬盘，其中 4 块硬盘做 RAID5，一块硬盘做 Hot spare，这样可以保证阵列柜在两块硬盘发生故障时，系统还可以正常运行。

3、 供电安全

由于医院许多大型诊疗仪器设备启动时有瞬间高压、高磁场等，会对计算机产生影响因此我们要求院方做到中心机房的电源专线专供，同时采用功率足够大的 UPS。

4、 病毒防范

我们通过设置 VLAN 和要求院方安装网络版杀毒软件来防范病毒。

数据安全

我们采用数据备份来保证数据安全。

本方案我们采用冗余备份策略。1、利用 Veritas Backup Exec 9.1 软件将数据备份到磁带库中。Veritas Backup Exec 能为跨网络的服务器和工作站提供快速可靠的备份和恢复能力。我们利用 Veritas Backup Exec 的作业管理功能设置备份定时任务，每天进行一次数据库数据完全备份，每三个月进行一次系统的灾难备份。灾难备份能在数据库服务器崩溃时，避免重装系统，利用最新的数据备份使系统尽快恢复到运行状态。2、利用 MS SQL SERVER 2000 自身的备份功能，每天定时自动地进行一次数据完全备份，备份数据存放到另一台数据备份服务器 HP ML570 中，同时在 HP ML570 中设置一定时任务，对每天的备份数据进行一次完整性检测，这样可以保证备份数据是完整、可用的。

通过数据备份，能使医院在破坏数据的灾难事件中造成的损失降到最低。

计算机网络安全是一个系统工程，除了采用保障网络安全的技术外，还要加强安全教育和制度管理，因此我们强烈要求院方重视对各级计算机操作人员进行计算机网络安全的教育，并制定较为完善的计算机网络管理制度，如严禁非操作人员使用电脑；计算机中心指定专职系统管理员掌握服务器密码，每次更新或升级计算机软件必须有两人同时在场，并做好记录等。

在整个项目方案中，我们用于保障计算机网络系统安全的措施主要是设备的冗余、链路的冗余。采用冗余措施，除了可以避免单点失效问题，还可以增加网络带宽和实现业务流量的负载均衡。因此，保障计算机网络的安全性不仅可以保证网络服务的持续不中断，还可以更好地提高网络服务效率。

整个项目完成至今近一年，从系统运行的情况来看，整个方案是合理的，高可靠性的，院方也感到很满意。当然，方案中也有不足的地方，如 F5 BIG-IP5000 控制器存在单点失效问题；随着院方的网上挂号等业务的开展，本方案中没有考虑到内网与公众网相连的安全措施等。