Intranet 的规划及设计

杨乔林　李威　饶上荣　张颖　（中科院计算所　100080）

提要：本文主要介绍在规划一个 Intranet 时所要解决的主要问题，这就是网络通信带宽及其规划、系统的高可用性的设计问题、信息安全性问题、网络系统处理能力问题、如何降低系统的总拥有成本等问题。

关键词：Intranet　总拥有成本(TCO)　高可用性　群集系统　MIS 系统　软件构件。

1. 引言

Intranet 在全球的普及化发展，引发了政府部门、企业、机关单位的信息系统向 Intranet 迁移。已有的局域网设法改造成 Intranet；没有的在构造信息系统的同时就要建设自己基于 Intranet 的信息系统。那麼究竟在构筑一个 Intranet 时，要考虑那些问题，将那些问题解决好才能建立一个适应自己单位要求的高质量、低成本的 Intranet？概括起来，我们认为需要解决好以下几个问题：

* 通信网络带宽的需要及其规划。
* 网络服务能力及其分配。
* Intranet 系统的高可用性。
* 信息安全设计。
* 降低系统总拥有成本(Total Cost of Ownership).

下面我们将对这些问题逐一进行讨论。

2. Intranet 网络带宽需求分析及其对策

1995 年前，我国绝大多数的网络系统都是低速网络系统，以广泛使用的 10M 以太网为例，它的理论最高传输速率为 10Mbps，其实持续的传输峰值只有 3－5 Mbps，在一个以太网段中，当网段节点数大于 30 时，3Mbps 的传输率也难以维持。显然网络传输速率必须提高，才能满足传输速率上的客观实际需求。

对于一个网络系统的质量评估，速率并不是唯一的评估标准，所谓服务质量－QoS (Quality of Service)可以说是网络的综和评分标准。显然从事不同工作的用户，对网络系统有不同的要求，也就是说，不同的用户群体对网络具有不同的 QoS 标准。

不同性质的工作，不同的处理对象，网络带宽的要求差别很大，图 1 给出了一些常见的处理对象的网络带宽的要求。

在考虑 Intranet 网络带宽的时候，特别是考虑布线时，要兼顾 5～10 年后，企业业务的发展，对网络布线的要求。

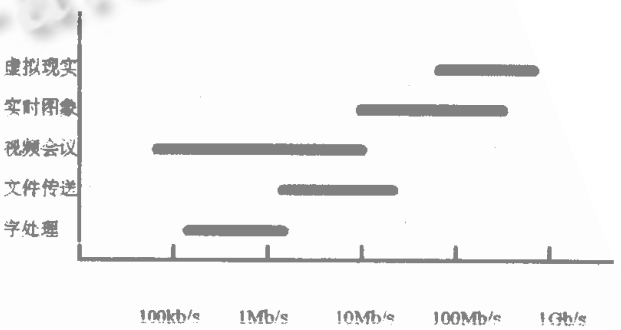

图 1　常见处理对象的网络带宽要求

解决网络带宽和 QoS 问题，可以综合地使用如下几种技术：

* 从 10 M 网络提升到 100 M 网络，甚至在网络主干上采用 1 G 网络技术。

根据本单位业务情况，考虑到并发事件的几率，参考图 1 的数据，可以估计本单位 Intranet 网络带宽的要求。

* 从网络共享技术转向交换技术。
* 网络分割技术。
* 从半双工转为全双工。
* 采用新的传输方式，例如使用 ATM，可将带宽提升到 155 M 或 622 M(根据 OC－48 规范将来带宽提升到 10Gb/s)。

例如，对于拥挤的共享 10M 以太网，利用网络交换和网络分割技术，在主干网安装 10M 或 100M 的交换器，使每个工作组都能共享 10M 或 100M 的带宽；若加上全双工技术，每个工作组便可获得 20M/200M 的带宽。

ATM (Asynchronous Transfer Mode) 是一种以信元

(长度为 53 个字节)为单位,在设备间进行信息传输的一种网络通信方式,它有如下特点:

* 信元载体可携带各种类型的信息,例如数据、视频、语音。

* 面向连接,通过 ATM 交换器,建立起源设备与目标设备的连接,可高速进行设备间的信元传输,具有较高的传输效率。

* 具有良好的可迁展性,网络支持不同速度设备的混合使用(从 1.5M 到 622M)。

* 可对 ATM 交换设备的传输时迟加以限制,因而对视频、语音等多媒体传送,具有较高的 QoS。

* 从 LAN 到 WAN 采用单一的技术,是一种可扩充网络技术。

虽然 ATM 的一些标准还在制定之中,但现有的 ATM 论坛标准在功能和互操作性等方面,已达到使用水平。

总之,ATM 是近年来发展起来的、能达 QoS 要求、扩展潜力较强、风险较低的组网技术[4]。

3. Intranet **服务需求及其对策**

在 Intranet 网络中,一般应提供如下的各项服务:

·DSN 域名服务
·Web 服务
·E - mail 服务
·工作流服务
·电子新闻服务
·FTP 服务
·Gopher 服务
·Telnet 服务
·数据库服务
·Transaction 服务
·远程访问服务(RAS)
·Proxy 服务
·特殊用途应用服务

对于这么多的服务进程,统统运行在一台计算机上,从投资和效果来考虑都是不好的。应该从网络服务的特点出发,分析各种服务计算机的计算能力,将这些服务适当地组合,分配在若干台计算机上。例如将数据库服务器、工作流服务器加上 E - mail 服务器,安置在二台计算机上,而剩下的其他服务器,安装在第三台机器上。对于工作繁琐的远程通信服务器,一般也配置一台低档的服务器或使用专门的远程访问服务器。对于一些使用 CAD/CAM 工具的企业,经常运行一些计算量很大的应用程序。在这类企业的 Intranet 网络中,配置一台大型的主机或高性能的工作站,专门地负责全企业高强度运算,并使整个企业共享它的处理能力,这也是一种非常经济的网络服务配置方法。

目前,前述的各种服务都可以安装在 UNIX, Windows NT, OS2 Wrap 等服务器平台上。由于 UNIX 发展历史较长,经过千锤百炼,在可伸缩性(多 CPU),服务器群集性能,容错与恢复性能以及 I/O 性能等方面,还具有一定的优势,因此,关键任务计算、高强度计算、高安全性系统等,还较多地选用 UNIX 服务器。但近年来 Windows NT 发展较快,在使用方便、低价位、用户熟悉等方面,具有较大的优势。而在可伸缩性(多 CPU),群集性能等方面,也在积极追赶 UNIX 系统,因而使其越来越多地占据更大的市场分额。

4. Intranet **的信息安全问题**

实际上 Intranet 不可能是一个信息孤岛,为了信息的沟通,不可避免地连通 Internet 网,另外还可能通过电话交换网接入远程用户。这样信息安全也是一个十分重要的问题。要解决信息安全应该从三方面着手:

·选择满足安全需求的服务器平台
·建立防火墙等安全措施
·严格执行安全的规章制度

为了建立一个信息安全的 Intranet 系统,对外、对内都应该有达标的安全措施。首先服务器平台、网络操作系统应选择都能满足需求的安全措施,这是最根本的一条安全措施。目前 UNIX, Windows NT 等都达到 C2 级的安全标准;而不能选择 Windows 95 等没有安全控制的操作系统,作为信息安全的服务器平台。同样,即使选用了 Windows NT 作为服务器操作系统,但在安装时,不选用 NTFS 而使用 FAT 作为它的文件管理系统,由于文件系统缺乏保护措施,也将是信息安全的大漏洞。

在 Intranet 与 Internet 连通时,为了保护企业信息的安全,必须设置硬件/软件相结合的防火墙。目前一般防火墙采用如下二种保护措施:

·包过滤
·代理服务

包过滤是对于进进出出的信息包都要进行适当的检查,将那些来自认为不可信的地址的信息过滤掉,不予以处理,而达到信息安全的目的。

代理服务是指对于企业内部与外部间要处理的事

物，都采取代理制的方式进行，而不是在 Intranet 内部，运行由外部直接控制的命令或程序。

即使对于一个在信息安全方面设计与实施比较完善的 Intranet，如果没有制定和严格执行相应的信息安全规章制度，信息安全的目标也是不能达到的。对口令长度的规定、口令文件的保存、口令更新频度等规定以及规定是否严格执行，都对 Intranet 信息安全性有重大的影响。

5.**高可用性 Intranet 系统规划**

在一个 Intranet 系统中，包含了数量众多的网卡、接插件、电缆、Hub、路由器、交换器等网络器件，数量众多的工作站以及数量不多但属全局性的各种服务器。经验告示我们，网络器件一般可靠性都比较高(著名厂家产品可用性可达 99.999%)，很少发生故障；工作站的数量很大，很容易出现故障，但其故障是局部性的，不会引起整个网络的瘫痪，而服务器则不同，当某个服务器出现故障时，整个网络都丧失它所提供的功能；尤其是数据库服务器出现故障时，可能引发数据丢失，使数据的正确性、完整性遭受破坏，因而其可靠性是很重要的。

通过长期观察，人们发现服务器故障主要来源是：

·系统挂起(一般是由硬件、软件故障引发服务器操作系统或网络操作停机)

·交流电源(电源掉电、电流波动等引起的故障)

·磁盘驱动器故障

·内存错误

为了提高系统的可用性，对于这四类故障；应分别采用相应的解决方法，例如利用服务器自动启动程序，当检测到服务器/网络停机时，自动重新启动网络系统或服务器系统；为了消除电源方面的故障，内部采用冗余电源，外部使用 UPS，并对电源进行有效的管理。对于最后两种故障来源，使用 RAID 和 ECC 内存，是行之有效的解决方法。但即使是使用了上述的多种措施，一台服务器的可用时间也只能达到 99.90%—99.94%的水平。

所谓可用性一般的定义是：

可用性 = (可用时间) / (可用时间 + 不可用时间)

对于一个具有 4 台服务器的 Intranet，假定每台服务器的可用时间是 99.93%。因而四台同时可用的几率为：99.72%。对于 24 小时开机的企业，平均全年不可用时间将达 25 小时。由此可知，平均每天不可用时间将为 4 分钟。根据企业业务的要求，可能还需要采用其他措施，将系统的可用时间进一步提高。

这里可以选用下列两种不同系统，一种是完全冗余系统，另一种是高可用系统。对于完全冗余系统，由于它在器件级进行冗余，这样经济上的代价特别大，如果不是绝对不能间断的系统，都不会利用这种系统。高可用性系统是在系统级进行冗余，因而成本相对较低。但系统需要化费一定切换和恢复时间，因而在微观上看来，它不是不间断的，但间断的时间不长，一般也在 3 到 5 分钟之内，对于一般企业的业务，不会造成很大的影响。

群集(Clustering)技术，是目前实现高可用性系统采用最多的方法。无论在 UNIX 或在 Windows NT 中都使用它。不过在 UNIX 系统中，它已研究开发多年，在伸缩性和可用性方面比 NT 来得更好些。

在几台服务器之间，实施群集技术时，一般都让它们两两共享一定相同的 RAID 磁盘。而通过网络或专线联结，检测是否出现工作异常的服务器，一旦这种情况出现时，群集中另一台服务器将替代它，为 Intranet 提供相应的服务。利用这种群集技术，服务器的可用性可提高到 99.95%以上，即平均每天停机时间降至 1 分钟以下。

6.**降低 Intranet 系统总拥有成本**(TCO)

对于台式机的总拥有成本，在国外已有较多的讨论，并取得了很大的进展。总拥有成本(Total Cost of Owership)主要除了系统初始硬件、软件费用外，还需要加上其他额外的费用，如维修费、支持费等。其中支持费种包括了升级费、培训费和网络管理等项费用。

对于不同的顾问公司，对于 TCO 估算差别较大，一般认为每年额外的费用在初始硬件、软件投资的 0.3 到 1 之间，是一个相当可观的开销。NC(Network Computer)、NetPC 以及各种瘦型客户机的倡导，零管理视窗(Zero Administration Windows)和远程管理/远程引导系统的设计，都是围绕降低台式系统 TCO 而展开的。

这里我们强调的是利用软件构件，在 Intranet 环境中，通过统一的客户图形界面，软件构件的可复用性和特殊的软件部署配置方式，以达到降低总拥有成本的目的[2][3]，这种方式有如下的特点：

(1)这些软件构件符合 DCOM 和 ActiveX 规范.

(2)利用这些软件构件，构成一种分布的网络信息系统：在客户机上运行客户图形界面也就是 Internet 流览器的界面；在工作流服务器上接收或分派任务；通过 Web 服务器或应用服务器获取数据库服务器上的相关信息；委托应用服务器上进行高强度运算任务等等。

(下转第 17 页)

(上接第 7 页)

(3)在整个网络系统中各种软件构件只需一份拷贝,保存在它运行的服务器中,而不是象现行的系统那样,同一软件需要安装在所有的机器中。

(4)软件缺陷的改正,软件的升级只需在运行该软件的服务器中运行,无需象现行的系统那样,在客户机中重新安装,因而降低系统的软件支持费用和提高了系统的利用率。

显而易见,利用这种结构的软件构件来构筑 Intranet 应用软件,不但可以降低软件开发费和支持费、用户培训等项费用,而且也提高了 Intranet 系统的利用效率。

采用具有代理功能和缓存功能的服务(例如 Proxy 服务),作为 Intranet 与 Internet 之间的统一通路,使用合理的安全配置,便可大大提高 Intranet 的安全性;利用它的缓存功能,将访问过的网页保存下来,当 Intranet 中另一个用户再次访问同一网页时,只需从 Proxy 的缓存区中取出,从而减少通信量,降低 Intranet 出口带宽的要求,节约了 Intranet 的建设和运行成本。

参考文献

[1] Cisco System:"Networkers'97"1997

[2] 李威、杨乔林:"Intranet 中基于软件构件的企业分布计算",计算机系统应用 1998.2

[3] 李威、杨乔林:"用于 Intranet 分布计算的 ActiveX 构件特性",计算机系统应用 1998.2

(来稿时间:1997 年 11 月)