

变压器产品辅助设计网络的建立及应用

李 维 (保定变压器厂计算中心)

一、引言

在当今局域网产品中,NOVELL公司的 Netware 以其开放式系统结构及优良的性能占据了广泛的市场:网络的各个工作站充分共享了昂贵的硬件及软件资源,节省了开支,提高了效率;严格的保密措施防止了用户的非法操

作;广泛的网络互连性确保了不同操作系统的工作站共享客户/服务器资源。但是,众所周知,NOVELL网络在国内大部分都是应用于数据库的管理,而在CAD领域的应用寥寥无几,许多CAD用户的微机处于单机运行状态。这样做有几个缺点:

其一,浪费了硬件及软件资源(绘图机、打印机及

CAD 软件不能共享);

其二,不利于统一管理,由于不能对用户的存取权限进行控制,容易发生图纸失密;

其三,无法实现异种机的互连,不能架起微机与主机 HOST(例如 IBM 93 系列、IBM 43 系列、VAX 系列)的桥梁,使微机不能利用主机的资源。

基于以上几点考虑,我厂于去年年底建造了一 CAD 绘图网,我们在建造这一网络的过程中遇到许多问题,经过多次探索,一一加以解决。下面对网络软硬件配置、网络环境等等作一详细介绍。

二、网络的软硬件配置

硬件的基本配置为服务器一台:COMPAQ 486 DX 33,4M 内存,硬盘容量为 540M;

工作站十台:386 DX / 33 兼容机;

ROLAND DXY-2200 绘图机一台;

3KV 不间断电源 UPS 一台;

NE 2000 兼容网卡;细同轴电缆;

IBM 3270 仿真卡一块,用来实现与我厂 9377 中型机的联机通讯。

网络操作系统为 Netware 3.11,20 用户;

工作站操作系统为 DOS 5.0;

CAD 应用软件为 MICRO CADAM V2.0, CCS V2.0。

三、网络的安装及其安全性

由于我厂设计处普遍使用 MICRO CADAM 2.0 软件作为绘图工具,而此软件不是网络版本,这就需要进行重新配置。我们将服务器硬盘分为两个卷:SYS 卷和 USER 卷,其中 SYS 卷中有 NETWARE 操作系统文件及一些用户可用的公共文件,自动分配为 F 盘;而将 CADAM 软件装入 USER 卷中,系统入网底稿文件将其映射为 G 盘,只需在服务器中装载一次,就可供各工作站共享。在这样装载完后我们遇到这样一个问题:G 盘中的 CADAM 不能起动,经过分析认为:MICRO CADAM 2.0 需占用约 600K 左右的基本内存,它不能识别扩展内存或扩充内存,由于 NETWARE 中运行 IPX/SPX 协议的 IPX.COM 文件和用于信息重定向的工作站 SHELL 文件 NET5.COM 需驻留内存,共占据了

大约 60K,加上 DOS 的常驻内存部分,只留下 580K 的基本内存,造成 CADAM 运行时的内存不够。为解决此问题我们使用 Quarterdeck 公司的扩展内存管理软件 QEMM386,将 DOS 移往高内存区 HMA,腾出大约 50K 的基本内存,用扩展内存工作站信息重定向文件 EMSNETX.COM 取代常规内存工作站信息重定向文件 NET5.COM,使占用的基本内存量由 NET5.COM 的 41.1K 降低到 EMSNETX.COM 的 8.9K,再将 MOUSE 等常驻内存程序移往上存储块 UMB,经这样处理后,空闲出 600K 左右的基本内存,CADAM 可正常起动,但还有一些细节问题需要处理,其中包括 CADAM 运行时要产生一些临时文件和日志文件,对这些临时文件和日志文件要将其放入本地驱动器,而不能是网络驱动器,具体可用环境设置命令 SET 来实现。

即 SET TEMP=C:\TEMP\及 SET JOURNAL=C:\MCADAM\;

可在本地驱动器 C 上建立空的临时文件目录 TEMP 和空的日志文件目录 MCADAM,供网络上的 CADAM 软件使用存放临时文件和日志文件,每次 CADAM 正常结束后这些文件都被自动删除。

由于 CADAM 对图形文件采用目录管理方式,图形文件必须放在 CADAM 称其为组的目录中,组的下面可以有若干子组。这就给我们带来了方便,可将设计处同一设计组所绘的图形文件放入一个目录,即 CADAM 的组,各个部件图放入其下的子组,不同的设计组对应不同的目录(CADAM 的组),便于图形的检索,但是在单台微机上运行 CADAM 不能控制非法用户对图形的存取和破坏,容易因病毒泛滥或人为误操作而造成整个绘图系统的瘫痪,还可能发生图纸的失密(非法用户对自己无权知道的图形进行查看或拷贝),给企业带来不可估量的损失。

NETWARE 通过对目录和文件的访问权限加以限制,分配文件和目录的属性等措施,避免了上述缺点,这样我们就可将 CADAM 软件装入网络服务器,经过精心地分配目录权限和属性后,可完全控制非法用户对图形的访问。例如可将设计一组所有用户所绘的图形放入 D1 目录下,将设计二组所有用户所绘的图形放入 D2 目录下,分配一组所有用户对 D1 目录下的图形有读(R)、写(W)、建立(C)、擦除(E)、修改(M)等权限;二组所有用户对 D2 目录下的图形有读(R)、写(W)、建立(C)、擦

除(E)、修改(M)等权限,这样两个组用户只能对各自目录下的图形存取,不能存取甚至查看对方图形文件。对一些特别需保密的图形,可将其放入特别目录,只将其访问权限分配给有权知道的用户,达到了保密的目的。以上只是从用户角度考虑图形文件的安全性,还可从文件和目录角度出发,对其设置特殊属性,例如,禁删除(D)、禁拷贝(C)、仅执行(X)等,从两方面达到文件的保密,我们对网络上的 CADAM 软件就设置了这些属性,防止了用户对它的误操作及非法拷贝。

四、网络的病毒防护

由于网络各结点间信息的频繁传输,也给病毒的泛滥提供了比单机运行更多的传播方式。病毒一旦在网络上泛滥,后果不堪设想。根据 DATAQUEST 公司的研究,即使病毒在网络上被清除之后,85%的网络在 30 天内会再次被感染。这就意味着一旦发现病毒,即使病毒被清除,其潜在的危险性也是巨大的。目前市场上的许多抗病毒软件,对网络尤其是对服务器的保护效果不佳。在这里介绍一下我们装载的专用于 NOVELL 网络的防病毒软件——LANPROTECT。

美国 TREND 公司的 LANPROTECT 是针对 NOVELL 网络的抗病毒软件,它以 NETWARE 可装入模块(NLM)方式运行于 NETWARE3.1 或以上版本中,LANPROTECT 已被 NOVELL 实验室测试和认证,广泛用于 NOVELL 网络的防病毒保护中。LANPROTECT 的主要特色如下:

LANProtect 软件主要包含三个部分:扫描器、用户接口、Netware 接口。

1.扫描器使用“深度扫描”算法进行文件的扫描,所谓“深度扫描”,是 LANProtect 的一大特色,即不扫描整个文件,而通过转移指令精确测定病毒在被感染文件中的位置,此技术的应用使任何长度文件的扫描时间不超过 50 毫秒,其快速和有效的特点非常适合于网络中庞大的文件系统。而且对一般辑毒软件不能发现的“变形病毒”有特殊扫描效果。

2.用户接口使网络管理员可对 LANProtect 进行预配置及调度,设定扫描时间和频率,被扫描的卷和目录,对 LANProtect 的加锁解锁功能,被扫描的文件类型及发现病毒后通知的 Netware 用户组等等。

3.Netware 接口不断监测网络的文件的传送,即工作站和文件服务器之间通过电缆(粗或细电缆,双绞线)共享信息时,LANProtect 的实时扫描器就被起动,扫描器对进出的文件通过“Deepscan”技术进行扫描,一旦发现病毒,随时报告网络管理员。

由于 Netware 操作系统取代了 DOS 的中断向量,大多数的病毒在 Netware 环境下不能运行,这就大大减少了病毒对 Netware 的攻击,但是,仍有一些病毒能以 Netware 的可装入模块(NLM)方式运行于网络中,一般扫毒软件对此无能为力,而 LANProtect 可识别至今为止 Netware 发现的所有病毒。通常网络管理员最头疼的是病毒的来源,由于不知道病毒从那个工作站侵入,以至于即使清除了病毒,在一个月网络又被感染。而 LANProtect 可解决此问题,它保持每个文件的传输轨迹,一旦在网络传输过程中发现病毒,马上报告病毒的来源,给出清除手段,把再次感染网络的机会降到了最低限度。

LANProtect 出色地实现了对网络服务器的保护功能,在 LANProtect 的保护下,即使网络上的每一工作站都被病毒感染,服务器仍然不会被病毒侵蚀。

LANProtect 也有其不足之处,即不能对工作站加以保护。但 TREND 公司的另一软件 PCCillin 弥补了其不足,它可实现对工作站的完整保护,PCCillin 首先将系统 Boot 区及分区表等重要信息存储在硬件加密盒中,此硬件加密盒插在并口上,由 EEPROM(电可擦除的 ROM)组成,病毒不可能侵入到此硬件加密盒中,当 Boot 区及分区表等重要信息被病毒破坏后,可随时将硬件加密盒(EEPROM)中的信息写回来覆盖病毒区。其次,PCCillin 驻留内存,随时监督系统运行状态,对硬盘 Boot 区,分区表加写保护,对软盘 Boot 区进行检测,防止非正常文件的内存驻留、非正常文件的打开及建立等等。当然,也可使用其它软件如:CPAV、NDD 等等将工作站 Boot 区及分区表存储在软盘上,用 VSAFE、VWATCH 等监视病毒。

总之,二者的结合是保护 NOVELL 网络的有效途径:LANProtect 安装在服务器上,实现对网络服务器的保护;PCCillin 安装在工作站上,对工作站进行保护。

我们在服务器上装载了 LANProtect,在工作站安装了 Pccilin,自安装辑毒产品以来,对网络病毒的蔓延控制良好,有效地预防和控制了网上病毒的人侵。曾有台

工作站发现“VDEFEND-1”和“VDEFEND”病毒。这两种病毒繁殖相当快,在20分钟内,大部分子目录中的可执行文件均被感染,系统已遭破坏无法自举。经传输系统和 LANProtect 处理后,工作站正常。我们曾尝试 CPAV 和 SCAN V95 以及 KILL V50.0 产品不能处理这种病毒。另有一台工作站上发现“DIR2”,经 LANProtect 处理正常。这两个事例均由 LANProtect 监视到工作站异常后,及时采取措施,病毒传播才得到控制,至今网络运行正常。

五、绘图机、打印机的共享

提供共享资源是网络服务器的重要任务,CADAM 作为软件在服务器中实现了共享,可供各工作站同时使用,绘图机、打印机等硬件也能共享,而不必每个工作站配备一套。

NETWARE 对网络共享打印机的管理借助于打印队列和假脱机 SPOOLING 技术实现,类似于大、中型计算机的主机对各终端用户所提供的打印服务。打印队列用来管理各打印作业的流向,SPOOLING 技术借助于打印队列,将某工作站上要打印的数据全部捕获,构成一个打印作业,然后再将该打印作业放至相应的共享打印机所对应的打印队列中去排队。采用了打印队列和 SPOOLING 技术后,共享打印机按一定的顺序先后为多个工作站的打印作业服务,不会出现混乱。且打印机忙时其它要打印的工作站不必空等,只需将自己的打印作业交付打印机队列参加排队,便可作其它的工作。

由于我单位的 NOVELL 网络主要用于绘图,绘图机的共享便成为硬件共享的主要任务之一,NETWARE 对打印机的共享提供了 NPRINT 命令,但对绘图机却没有提供任何直接的命令,我们所见的资料上也无此介绍,如何共享绘图机成为一个棘手的问题。经分析我们发现 NETWARE 可以截获应用程序发送给本地打印机端口的数据,并将其重定向到指定的打印队列或将其存入指定的文件中,利用此功能可实现绘图仪的共享。

首先,我们将 ROLAND 绘图仪连结到服务器的并口,用打印作业管理程序 PCONSOLE 命令建立打印服务器 PS1,并在 PS1 上建立打印队列 PLOT_QUEUE,即为存放绘图数据的队列。在服务器控制台方式下,安装并启动打印服务器 PS1。再将网络服务器中共享的

CADAM 软件的绘图仪输出配置为 HP 7580,驱动程序为 HPGL.SYS,发送到第一个并行口,当各个工作站调用网络服务器中的 CADAM 提交绘图时,绘图数据都发送到了各自本地的第一个并行口 LPT1,再用 NETWARE 的命令 CAPTURE 设置截获发送到 LPT1 的数据,将其重定向到前面建立的打印服务器 PS1 上的打印队列 PLOT_QUEUE,连结到服务器并口的 ROLAND 绘图仪即可将提交的图形绘出。

在共享绘图机的基础上还可安装共享打印机,原理与前面相似,都是截获应用程序发送给本地打印机端口的数据。由于本地的打印机端口 LPT1 已被截获到绘图队列 PLOT_QUEUE,对打印机可截获应用程序发送给本地打印机端口 LPT2 的数据,将其重定向到另一个队列即打印队列 PRINT_QUEUE,由于服务器只有一个并口已分配给绘图队列 PLOT_QUEUE,只能将此打印队列 PRINT_QUEUE 对应某一工作站上的一个并口,此为远程共享打印机方式,为此,服务器控制台上应依次执行下列命令:LOAD REMOTE;LOAD RSPX;LOAD PSERVER PS1。联结远程共享打印机的工作站应执行下列命令:RPRINTER PS1 1。这之后,任何工作站发往本地 LPT2 口的数据,都将被送往远程共享打印机打印。即任何工作站用户键入如下命令:TYPE 文件名 >LPT2 其要打印的文件都将被送往远程共享打印机打印出来,即使工作站上物理上只有一个 LPT1 口,无 LPT2 口,也无任何妨碍,仍然可正确打印,不会出现写设备错误的情况。

六、工作站与 IBM 9377 中型机的联机通讯

NETWARE 提供了 PC 机与 IBM 主机联机的手段,借助于 NETWARE SNA Gateway 这一软件产品,可将 NETWARE 网络与我厂的 9377 中型机连结,连接后允许网络上的 PC 工作站仿真主机终端,使用主机的程序和数据,并且主机可以向下把数据加载给网络。这些任务将在我们明年的工作中完成,但现在我们已经在网络的其中一台微机工作站上通过 3270 仿真卡实现了与 9377 中型机的联机通讯,此单台微机可仿真主机终端,实现文件的双向传递,但无此 3270 仿真卡的工作站却不能与主机通讯,只有借助于 NETWARE SNA Gateway 这一软件,才能实现此功能。