国际集装箱码头的网络规划

摘要：

企业信息系统的建设是一项复杂的系统工程，它包含了网络、主机、服务器、操作系统、数据库、应用系统等多个组成部分。网络系统是整个系统信息交换互联的基础平台，如何构建一整套“稳定、高效、安全”的网络系统是在进行信息化建设中所要面对的首要任务。尤其是新建企业网络规划的好坏，将对企业未来信息化发展起到至关重要的作用。本文主要是针对国际集装箱码头公司的组建过程中，结合实际情况，展开网络规划和设计。由于初建企业的办公环境、机房环境的不确定性，网络规划带有很大的风险，如果贸然作一次性大的投入，势必会带来不小的损失，因此本文作者采取了分几步走的策略来减少风险。本文中涉及的网络规划从三个阶段展开，这三个阶段分别为第一阶段（先筹建阶段）、第二阶段（筹建期—投产初期）、第三阶段。本文分别详细的阐述了各阶段的任务和相关的网络规划工作。

正文：

2008 年 1 月**港欧亚国际集装箱码头有限公司开始筹建，该公司有三家香港上市公司共同出资成立。其码头岸线长 1100 米，承台宽 73 米，将建设 2 个 10 万吨级和 1 个 7 万吨级集装箱泊位，设计年吞吐量为 170 万 TEU。主营业务为集装箱装卸及运输、集装箱货代服务等物流服务。因为公司信息系统对整个公司的业务有着重要的地位，因此信息系统网络建设随着公司筹建同时进行。我为该公司信息技术部部长，负责整个信息系统的规划和建设工作。由于目前处于建设筹建期，办公环境和网络环境都不能确定。针对目前的实际情况，在对公司信息系统进行网络规划过程中，将划分为三个阶段分布实施。

1. 第一阶段（现筹建阶段）

筹建期间，我们公司办公位于租用的办公楼中，公司的计算机数量才三十多台，这些计算机通过内部交换机组成一个局域网，通过一条 ADSL 链路连入 Internet，在网络出口处没有加装任何网络安全设备，内部网络完全地暴露在外界，也就可能受到各种有意或无意的攻

击。因此在目前情况下，我们公司所有计算机存在着极大的安全隐患。

现阶段的主要问题是网络安全，为了不影响各部门计算机的正常工作，在这一阶段主要应做好如下工作：

（1）技术方面

采用正版化操作系统、正版化应用软件、网络防病毒软件系统并及时升级操作系统补丁，建立一个结构上较完善的网络系统。

通过及时、有效的补丁升级，能够有效防止局域网主机和服务器相互之间的攻击，降低现代网络蠕虫病毒对网络的整体影响，增加网络带宽的有效利用率。

网络防病毒软件系统由服务器和网络防病毒软件控制中心以及客户端软件组成，选择一台微机或应用服务器安装网络防病毒系统的服务器端软件，并通过 Internet 利用防毒系统的在线更新功能实时地进行病毒码信息的更新。网络中的所有计算机和服务器均安装防毒系统的客户端软件，利用服务器端获得最新的病毒码信息对计算机进行病毒扫描。这种方式虽然投资较大，但是对病毒码信息进行实时的更新，可以保证网络不受病毒侵害，控制病毒的大肆传播。

（2）服务方面

建立计算机使用管理制度、上网管理制度，建立操作系统以及防病毒软件定期升级机制、通过这些服务，增强网络的抗干扰性。

2. 第二阶段（筹建期--投产初期）

筹建期间，计算机技术的应用很大程度上还只是停留在单机应用的水平上，应用软件也只是办公软件和简单的数据库应用。随着企业信息化的逐步深入和企业自身发展的需求，在充分利用原有资源构建适合自身情况、满足实际需求的网络系统是非常必要的，也是切实可行的。这一阶段企业建设网络系统的主要功能是为了强化企业的管理、生产和经营，提高企业的生产效率，创造更多的经济效益。就我公司而言，这一时期网络规划应以业务系统为核心、以中心机房为中心，以最少的资金来构造适合我公司实际情况的网络系统。

下面从网络基础架构、Internet 接入、网络安全管理等方面进行阐述。

（1）网络基础架构

我公司网络架构由有线网络、无线网络和 GPS 系统组成。

从目前的网络技术和应用的发展趋势来看，采用基于 TCP/IP 协议组的以太交换网模式是最适合、也是必然的。以太交换技术和产品都十分成熟，网络的实现和管理都很简单，维护量也小，并且可以向未来的发展进行平滑的升级和过渡。

▪通信子网的架构

中心机房位于公司综合业务用房五楼，在中心机房设置核心网络设备选择千兆的以太交换机。所有的现场视频监控点、网络工作站和应用服务器通过无线网络方式或六类双绞线接入到交换机中构成一个集中接入的星型网络带宽。当中心交换设备需要由多个交换机构成时，可以选择堆叠的交换机，可堆叠的交换机之间进行交换时利用带宽很高的内部总线，可以保证每台接入的计算机都具有很高带宽。当工作站到中心交换设备的距离超过 100m 时，可以在工作站和中心交换机之间设置一台交换机，以级联的方式与中心交换机连接。

电话语音网络同上述近似。

在实际网络构建时，为满足应用系统及网络安全性的需求，我们将网络系统分为内部网和外部网两大部分来进行设计。内部网主要为内部业务应用系统提供网络平台，如码头操作系统、人事管理系统、财务管理系统、办公自动化、电子邮件等；外部网提供内部工作人员对外部 Internet 的访问，同时也是对外网站的网络平台。内部网与外部网之间采用物理隔离的方法来保证安全性。在内部网络中通过 VLAN 技术可将各应用系统划分为相对独立的网络。

（2）服务器的选择

服务器是网络的重要组成部分，服务器的性能往往决定了网络应用的性能。由于网络产品的功能、性能与价格是成正比的。因此，要根据具体的需求和应用程度来选择服务器。对于极为关键业务的数据库服务器选择小型机加磁盘阵列，Web/Mail 服务器通常选择性能较高的企业级 PC 服务器，而 DHCP/WINS 服务器、防病毒服务器、DNS 服务器和代理服务器由于工作负载较小，用配置较高的 PC 或部门级的 PC 服务器来担当就可以了。

双机集群是目前大多用户采用的高可用环境，简单的说就是两台服务器加一台磁盘阵列，通过软件实现双机环境。集装箱码头的工作性质的特殊性要求其信息系统 7 天 x 24 小时不间断运行，决定采用双机热备、远程容灾方案为码头业务系统提供高可用解决方案。

（3）数据库的选择

经过多方比较 Oracle 11g 在系统性能、稳定性、操作性均优于其他版本，因此我们选择 Oracle 11g。

（4）Internet 接入

对 Internet 资源的访问，最终都是通过资源所具有的惟一的公有 IP 地址实现的。对于一个内部网络，每一台工作站和应用服务器的 IP 地址均为内部专有的地址，以这样的 IP 地址是不能访问 Internet 资源的。因此，要实现一个内部网络对 Internet 的访问，必须在内部网络和 Internet 之间设置一个具有网络地址转换功能（NAT）的设备。

对于从内部网络向外发出的 IP 数据包，NAT 设备可以将数据包中所包含的源 IP 地址和源下 TCP/IP 端口号等信息转换为可以在 Internet 上使用的公有 IP 地址和可能改变的 TCP/IP 端口号；而当 Internet 主机响应的数据包流入内部网络时，NAT 将数据包中包含的目的 IP 地址和目的 TCP/IP 端口号等信息转换为专有 IP 地址和最初的 TCP/IP 端口号，从而对外部屏蔽了内部网络的 IP 地址。

在一台计算机上安装相应的代理软件作为代理服务器，由代理服务器执行地址转换的功能。

（5）网络管理

在第一阶段安全建设的基础上，进一步增加网络安全设备，采纳新的安全服务和技术支持来增强网络的可用性。

- 技术方面.增设局域网防火墙、采用入侵检测、邮件防病毒软件、动态口令认证系统、并在重要客户端安装个人版防护软件。
- 服务方面，建立中心机房管理制度、对服务器进行定期扫描与加固、对防火墙日志进行备份与分析、对入侵检则设备的日志进行备份、建立没备备份系统以及文件备份系统。
- 支持方面，要求服务容提供灾难恢复、实时日志检索、实时查杀病毒、实时网络监控等技术支持。要求服务商提供故障排除服务，以提高网络的可靠性，降低网络故障对网络的整体影响。

3．第三阶段

这一阶段计算机网络架构已经完成，采取的措施以进一步提高网络效率为主。这一阶段的重要任务是在原有网络的基础上对生产业务、对新网络技术挖潜创新。如将公司的网站建设成为商务网站，直至实现收费功能。

4．进一步的工作

目前我们还有许多值得完善的地方，下面将是我们下一步的网络规划：

（1）技术方面，采用反垃圾邮件系统、网络管理软件、OOS 流量管理软件。

（2）服务方面，采用白客渗透测试，要求服务商定期提供整体安全分析报告。

（3）支持方面，要求能够实时或者时候查找攻击源。

随着新技术、新产品的不断涌现，网经技术的不断发展，对于网络安全的要求不断提高，这就要求我们的网络还要不断改进，不断增强。