



## 北京烟草行业计算机广域网的设计和实现

何翔 薛建国

北京烟草专卖局 经济信息中心, 北京 100029

**摘要:** 详细论述了北京烟草广域网的设计思想, 并结合网络系统的开发和实施, 探讨技术的选型, 平衡网络的先进性和实用性、保证稳定可靠等、阐述了网络的安全保障措施, 最后分析总结了网络特性和效果。

**关键词:** 烟草 信息 网络 技术 设计

随着烟草信息化时代的到来, 信息的价值已被企业所认识和接受, 为适应烟草行业“电话订货、网上配货、电子结算、现代物流”现代流通体系建设, 北京烟草加快建立了自己的信息化网络, 以提高企业的管理水平, 完善企业的内部机制, 提高企业的效率, 达到世界先进水平和国际接轨, 增强市场的竞争能力, 获取更高的经济效益的目的。

### 一、应用背景

经过“九五”期间的信息化建设, 北京烟草行业的计算机硬件数量从最初的几台已发展到百余台, 运行方式从单机运行发展到可以进行电话拨号传输, 但其传输速度和安全性等各方面不能得到保证。从计算机和信息化发展的水平和市局(公司)最新的经营管理理念以及“十五”网建规划对整个信息网络建设的要求来看, 当时市局(公司)的计算机网络仍处于一个起步的、不完善的阶段。

根据北京烟草实施“三大工程”建设新要求, 加快北京烟草信息化建设的步伐, 有必要尽快建立一套快速、高效的北京烟草广域网系统和基层单位网络子系统, 实现销售专卖等各种信息的合理组织、流动, 提高市局(公司)经营、专卖、管理的整体水平。

### 二、网络设计思路

根据北京市烟草专卖局目前的需求和未来的发展, 在设计和建设北京烟草行业网络中, 我们坚持全局统一规划, 既做到与北京烟草信息化长远发展相适应, 又坚持分步实施、稳步实施的策略。将计算机网络建设成一个起点高、安全可靠、易于扩充和升级、便于管理和使用的网络系统。具体包括:

1. 坚持严格按照国家烟草专卖局制定的行业信息网的建设原则和标准进行设计。
2. 网络系统应充分考虑现有的网络设备的使用, 并保持与相关国际标准、国家标准以及主流操作系统、网络协议的兼容性, 体现网络的先进性。
3. 各局域网的信息能够及时、准确、透明地传输到决策、管理、生产和销售等部门, 各局域网之间相互沟通。
4. 建立一个负载均衡的网络系统, 要求其具有较高的可靠性、可管理性及容错性。
5. 具有很好的扩展性, 以备将来有支持多媒体信息, 如图像、话音、数据的同时传输的能力。
6. 信息中心是一个具有信息转发、信息存储共享、信息综合处理及查询服务能力的交换网络的核心, 为全局提供必要的信息服务。

### 三、网络技术设计

#### 1. 网络关键技术选型

##### (1) 广域网线路选型

专用线路为远程端点之间提供点对点固定带宽的数字传输通路，尤其在对速度、安全和控制要求甚高的WAN应用环境，是实现WAN连接的主要手段，其通信费用由专用线路的带宽和两端之间距离决定。由于各单位地距离不是很远，北京网通将提供宽带数字电路（SDH），不仅可靠性高、并且具有很好的性能价格比。因此在网络设计中我们选用SDH或DDN线路作为广域网的首选线路。

##### (2) 交换以太网技术

交换以太网是先进并比较成熟的网络技术。它在保证与以太网协议兼容的前提下，提高络利用率，减少网络资源争夺造成的冲突，使网络性能大幅度提高，以满足各类数据信息传输的要求。动态交换代表了当今交换技术发展的方向，所以在网络设计中采用基于动态交换技术。

千兆以太网是10Mbps以太网的1000Mbps版本，它仍与以太网采用同样的帧结构，千兆以太网相对其他高速网络技术更容易被掌握和接受，它可以应用在共享式和主干环境下，提供带宽的共享式网络或主干连接，同时也可以应用在交换式环境下，提供优异的服务质量(QoS)。千兆以太网与传统的以太网技术相似，同样遵循CSMA/CD协议，现有的以太网、与其它新型网络技术相比，更方便地使现有的10M、100M LAN无缝连接到1000MbpsLAN上。我们选择千兆以太网技术作为机关局域网主干的首选技术，各个局域网到桌面都采用了较高的性能价格比的快速以太网技术，不仅保护用户原有的投资。

##### (3) VLAN(虚拟局域网)技术

VLAN是逻辑上的网络，可以避免许多实际网络的缺点和限制。在同一个虚拟网络VLAN内部的成员属于同一个共享介质区域，可以相互连通；不同VLAN之间的成员是不可能直接进行相互访问的，从而可以满足实际生活中各机构管理的需要，使得日常的管理维护非常方便。我们利用VLAN技术，对不同部门或不同的服务性质划分，保证信息资源仅对合法用户开放，同时可以简化终端的删除、增加、改动，控制通信活动，保护工作组和网络安全。

##### (4) 第三层或多层交换技术

从网络用户的角度看，LAN通讯被分成两种等级的性能。数据包直接通过交换机进行传递时，享受着高速公路快速的、稳定的传递性能。但是那些被迫经过路由器的数据包只能使用慢速通路，当流量负荷严重时，会受到更严重的延迟困扰。多层（三层）交换技术正是交换技术和路由技术智能化的组合，它为各种结构的局域网提供一个完整的、集成的解决方案。

#### 2. 广域网设计

##### (1) 网络总体结构

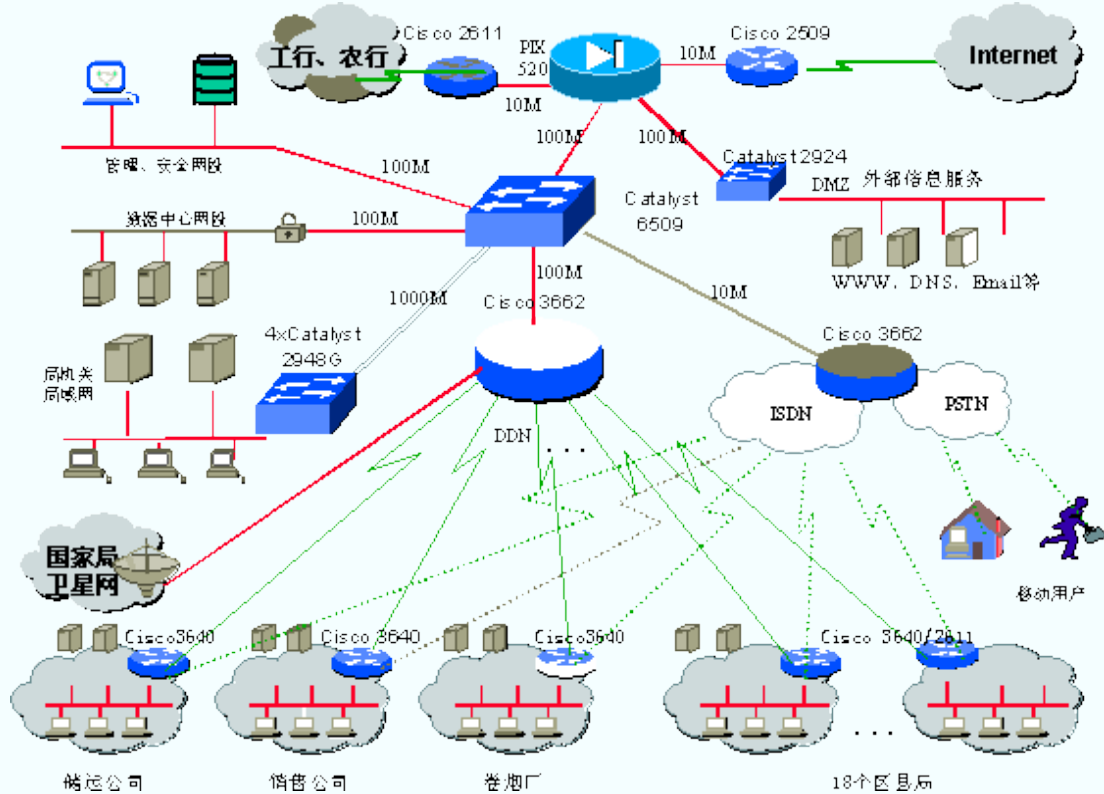


图1 北京市烟草专卖局计算机网络拓扑图。

北京市烟草专卖局主干网的拓扑结构是：以北京市局为中心的星型结构（参见图1）。北京烟草广域网是以北京电信SDH或DDN专线系统为基础，以市局信息中心为中心，将各二级单位局域网连接起来，同时考虑了线路和设备的备份。为了确保在现有和不断发展的通讯条件基础上，实现系统最大程度的互联性和管理性，在网络设计中统一采用一致的网络协议、路由协议和网络操作系统标准，建立了北京烟草的Intranet网络。

### (2) 广域网路由协议

在一个大型的广域网中，路由协议的选择主要取决于两个方面，一个是广域网的拓扑结构，另一个是路由协议的效率。我们在广域网中使用OSPF作为主干路由协议，OSPF是由属于IETF的IGP工作组所开发的，是为IP网络而设计的，成为一种标准的路由协议，被大多数路由器厂家支持，它不但具有较高的效率，而且具有可靠的安全机制和良好的开放性。

### (3) 广域网中心节点设计

信息中心是北京烟草广域网的信息交换中心，是所有二级单位网络出口信道的路由汇接枢纽，也是整个北京市烟草公司广域网络的控制、管理和维护中心。

汇接路由器用于信息中心与各二级单位的网络连接，由于其处于广域网的汇接中心位置，因此要求具有很高的包转发和交换能力、足够的接入端口种类和数量，并具有较强的管理控制能力等功能。为此在市局信息中心配置两台Cisco 3662路由器，既起到备份的作用，又确保负载均衡，其采用先进的体系结构设计，高的备板路由能力，具有很高的性能价格比，对语音图象等新技术有全面的支持。对于北京烟草这样大型的计算机广域网络，路由备份功能是不可缺少的，在网络设计中，在Cisco 3662上增加NM16-AM及NM-8B-S/T模块，ISDN线路或电话拨号网作为路由备份线路，以保证网络正常运行，减少瘫痪时间，它是降低经济损失。

### (4) 区县局（公司）等下属单位网络设计

各单位配置一台Cisco 3640或2611采用一个同步串口经SDH或DDN线路和市局相连。可以再配置一个ISDN接口作为路由备份。区县局等单位各配置一台Cisco 3640或2611路由器，作为广域网接入使用。Cisco 3640或2611是模块化结

构的。为其配置一个NM-2FE2W网络模块，提供两个快速以太网接口；为其配置一个广域网接口卡WIC-2T，采用一个同步串口经专线和市局相连。再配置一个WIC-1B-S/T ISDN接口作为DDN主干备份；为实现下属配送中心等单位的拨号访问接入，配置一块NM-8AM模块提供8条模拟PSTN拨号访问。

### (5) IP地址分配

北京烟草行业广域网IP地址是参照行业标准《烟草行业计算机网络建设技术规范》进行设计。下属单位根据其网络规模得到一个或多个C类网段的IP地址。

## 3. 局域网设计

我们在局域网设计上将信息中心网络和机关局域网融为一体，采用一套物理网络设备，采用划分不同虚拟网段VLAN的办法隔离相应的网络，完成不同的功能。具体参见附图4。

局域网设计采用星型结构，采用专为需要千兆扩展、高度适用、多层交换的主从分布而服务器集中的应用环境设计的Catalyst 6509构成高速、稳定的网络主干，其具有较高的数据交换能力、VLAN划分、第三层交换能力等性能，支持交换背板可扩展到256Gbps，多层交换速度可扩展到150MPPS，结合其IOS广阔服务功能，Catalyst 6509具备强大的网络管理性，用户机动性，安全性，高可靠性和对多媒体的支持，能满足企业的内部网（Intranet）苛刻要求网络服务（如ERP）和网络语音图象使用。为了保证系统的高度稳定，在主干交换机中分别配置冗余的主控（含引擎第三层路由模块）模块，这样主干交换机可以实现引擎、路由自动备份，保证系统的正常高效、运行。并根据需要划分成多个不同的网段：数据中心网段、管理网段、开发网段等。在机关配线间配置楼层交换机，采用两条千兆光纤Channel冗余上联主干交换机，保证了局域网的高可靠性接入功能。

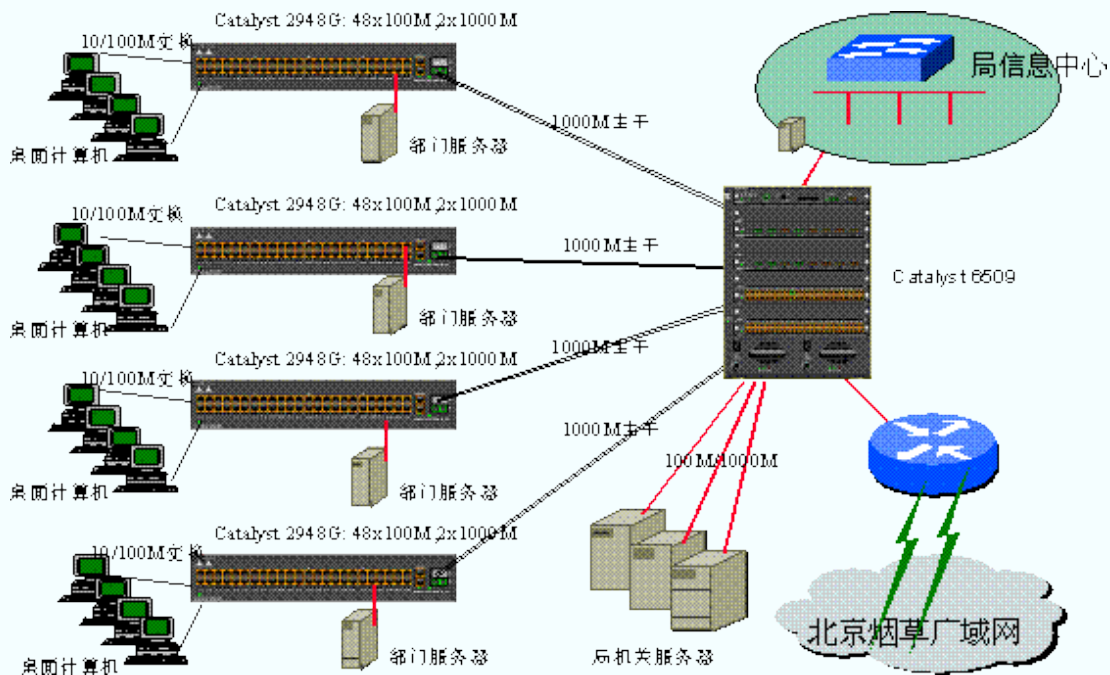


图4：机关局域网示意图

## 4. 网络安全的设计

### (1) Internet出口及防火墙区域设计

我们为北京烟草行业广域网设计统一的Internet出口，以确保对Internet访问的控制和保护内部企业网。在建立北京市烟草专卖局独立的INTERNET出口时，考虑到INTERNET的开放性，我们选用一台CISCO PIX 520作为独立INTERNET出口处的防火墙，在上面建立DMZ网段。其采用一种安全的、非UNIX系统的实时内核(kernel)，避免了以



UNIX系统为平台的“防火墙”技术所受到的攻击，支持多达16,000个同时链接；高达45Mbps的网络数据通过能力；安全的动态地址和静态地址翻译。

#### (2) 入侵探测IDS

我们采用IDS-4210 Sensor，服务于整个市局机关网络安全平台。实时进行入侵检测，对合法流量和网络来说是透明的对未授权或企图破坏的动作，中断其访问网络或中止企图破坏的连接，实时响应拥有综合的攻击签名清单，可探测出大范围的攻击，并能探测出基于内容及有先后顺序的连续攻击。

#### (3) 网络防病毒设计

根据烟草专卖局网络设计，我们选用Norton AntiVirus for Windows2K的解决方案，市局信息中心建立一个控制中心和一级防病毒服务器、每个下属单位建立一个二级防病毒服务器及各个客户终端构成。病毒定义码和扫描病毒引擎的更新由一级防病毒服务器及时分发，控制中心快速方便实现集中管理，对网络性能的影响非常小。

#### (4) VPN加密技术

考虑到IC卡电子结算系统等非常重要的数据传输的保密性，我们在本项目中采用的是56位的IPSec DES加密技术和防篡改技术，组建行业VPN网络，对双向流动的数据进行加密，传输的数据就可以得到有效的保护。

### 四、网络设计特点分析

在北京烟草广域网建设项目中，我们根据北京市烟草专卖局当前的需求和未来的发展，考虑全局，坚持长远发展规划，将计算机网络建设成一个起点高、安全可靠、易于扩充和升级、便于管理和使用的网络系统。北京烟草广域网系统具有5大特点：

#### 1. 重点突出技术先进性

本系统在满足实用性的基础上，起点高，在关键环节中选用了代表先进的网络技术主流先进产品，确保选用的产品具备良好的先进性、通用性和权威性，用户会获得较好的支持和保障，所设计的系统拥有较长的寿命。例如：CISCO公司的高端千兆交换机，千兆网以太网技术、VLAN技术、三层交换等技术，OSPF作为高效主干路由协议，建立一个技术先进成熟的网络。

#### 2. 具备高安全性和可靠性的特点

系统和数据的安全性的重要意义对于企业来说是不言而喻的，因此，本网络系统在数据的采集、存储、传递、交换和使用过程中都设置了相应的安全机制，确保了数据的正确性和可信度。例如：北京烟草广域网采用了VPN技术、网络防病毒、入侵探测IDS和防火墙。

系统可靠运行是整个系统建设的基础。我们在设计上要求各级网络均都具有网络监督和管理能力，并适当的考虑了关键设备和线路的冗余，能够进行在线修复、更换和扩充，建立健全了为防止异常情况所必须的保护性设施。

#### 3. 充分考虑了经济性和实用性

它采用了成熟的网络技术和设备及通信技术，同时兼顾了已有设备，充分利用了已有的资源，保护原来的投资；既能够满足北京市烟草行业现有的网络互连和各种应用需求，又对未来可能出现的新需求提供良好的网络支持。

#### 4. 具备很强的开放性的特点

北京烟草广域网总体设计采用了开放式的体系结构，使网络易于扩充和升级，对外界环境变化有很强的适应能力，支持与未来新的网络技术平滑过渡，能够根据北京市烟草专卖局(公司)未来需求的变化进行升级和灵活地调整。例如最近在北京烟草广域网扩容改造的工程中，只在线路上进行了容量扩容，而系统仅作小量修改就能在新环境下运行。

#### 5. 本项目支持多服务功能

北京烟草广域网能够传输多种数据信息、语音信息和图像视频信息，确保运行于计算机网络之上的视频通讯系统与应用系统之间彼此不受影响，例如刚实施视频会议系统传输的图象和声音都清晰，效果非常明显。

## 五、系统应用效果

一年多来，北京烟草广域网一直保持稳定运行，保证了卷烟访销配送系统、市局业务平台、集中式电话订货系统、IC卡结算和专卖管理系统等系统正常使用，为北京烟草信息化建设打下了坚实的基础，获得了良好的经济效益。特别保证了近期实施的国家局“一号工程”和北京烟草视频会议系统的运行，目前北京烟草广域网真正实现了视频（视频会议系统）、音频（电话订货系统）和数据传输的三合一，是一个真正具备了多媒体功能的网络系统，下一步网上配货、电子商务、现代物流、办公自动化等系统开发应用，广域网应用程度将得到了更大提升。

---

作者简介： 何翔，女，工学硕士，现为北京市烟草专卖局经济信息中心副主任兼总工程师、高级工程师，从事计算机、网络、管理信息系统工作。

www.tobacco.org.cn All Rights Reserved.

版权所有 中国烟草学会

本网站由中国烟草物资电子商务网提供技术支持