

# 银行网络规划与设计

李先红

湖南现代物流职业技术学院, 湖南 长沙 410131

李先红



李先红(1980-)  
男, 硕士研究生,  
研究方向: 计算机  
网络与通信; 网络  
安全。

## 摘要

银行网络建设项目是银行业务正常开展过程中很关键的一个环节, 其规划与设计的好坏将直接影响到网络的连通性、稳定性、网络的扩展性、网络的健壮性、网络安全性以及网络的性能, 从而直接影响到银行业务的正常开展及将来业务的拓展。商业银行的网络建设项目不仅为商行提供生产、信息化办公的平台, 要同时为将来商行各种基于数据、语音、视频业务的广泛应用打下坚实的基础。因此, 对于一家银行企业而言, 对网络进行合理的规划与设计就显得尤为重要。本文针对银行的业务特点, 结合工程实践经验, 从系统的需求分析、建设目标、银行光纤网络的具体设计、全网安全等多个方面对网络进行规划与设计。

## 关键词

商业银行; 网络规划与设计

DOI: 10.3969/j.issn.1001-8972.2014.08.048

某银行是一家区域性的商业银行, 随着企业业务不断的扩展, 企业规模越来越大, 客户的数量越来越多, 各类型的银行业务也在不断地拓展, 原有网络已不能满足其需求。该银行计划增加新的营业机构和离行式的自动柜员机(ATM)。该公司提出了将其银行网络进行改造和优化计划, 要求对该公司网络进行重新规划设计与改造。

## 1 系统的需求分析与建设目标

该银行的现有网络的具体结构如下: (1) 现有网络仅限于32个网点与中心之间业务数据传输; (2) 网点以64K的DDN为主线, ISDN为备线; 中心有两条E1链路和一条PRI链路; (3) 网点路由器采用Cisco 2611XM, 连接到中心设备; 中心由两台cisco 3662各连接一条E1线路, 并互为备为, 提高可靠性; 一台cisco 3640连接到PRI线路, 作为备份链路; 以两台cisco 4006作为中心交换机并互为热备; 中心端设置了ACS服务器, 进行认证, 实现网络的安全访问。(4) 网络主要采用EIGRP协议。

从上面的情况来看, 可见现有网络存在核心路由器处理能力较低, 广域网传输带宽过窄、可扩展性较差等缺点, 已不能满足该商行的业务扩展的需要。现提出网络改造的需求如下:

(1) 营业部及离行式ATM机的扩展需求: 该商行

将扩展为33个网点、增加60-120台离行式自动柜员机(ATM)与中心连接。

(2) 线路改造需求: 采用VLAN-VPN技术的光纤线路组网方式, 分别由电信和网通公司两家提供; 中心采用4条100M线路(两家公司各两条), 网点为10M、ATM为2M, 接口类型均为RJ45。

(3) 网络结构改造需求: 各网点保留主要线路即DDN线路, 撤销备份ISDN线路, 改为光纤线备份; OA、监控、测试网络等其它应用改走光纤线路, 无备份线; ATM只有一条光纤线路, 无备份线, 其上主要应用为业务和监控。

(4) 路由结构调整及网络安全需求: 接入端的各种应用相对较为隔离如设定为不同网段、运行在不同的VLAN、TRUNK上等; 在光纤上跑的业务数据流应加密; 网点上, 原有关于DDN线路的配置不变, DDN与光纤线路之间可以实现自动切换; 在光纤网上的业务数据传输走动态路由协议, 监控部分可设置一个大的局域网, 其他应用可根据实际情况采用动态或静态路由。

## 2 网络规划与设计原则

商业银行的网络建设项目不仅为商行提供生产、信息化办公的平台, 要同时为将来商行各种基于数据、语音、

视频业务的广泛应用打下坚实的基础。为实现网络高质、高交互的目标要求，在网络建设中始终坚持了以下建网的原则：高可靠性：网络系统必须具有高度的安全可靠性和，尤其是对商行的业务数据传输必须做到万无一失，通讯线路、关键设备必须具有备份措施。网络关键设备选用高可靠性网络产品、设备充分考虑冗余能力、容错能力、网络的自愈能力、可靠的备份策略等。技术的先进性和实用性为系统提供最佳的性能/价格比；高性能：保证网络的良好运行，保证各种数据（数据、语音、视频、图像）的高质量传输；同时还要考虑网络的可管理性；可扩展性；安全性等等；

为了切实达到以上的网络设计原则，使商行网络系统具有良好的扩展性和灵活的接入能力，并易行管理和维护，在网络设计及构建过程中我始终遵循了如下的技术策略：

统一平台、统一标准：要实现网络业务能融合到一起，实现数据、语音、视频业的融合，就必须统一标准。在具体实施中，必须统一规划IP地址及各种应用，采用开放的技术及国际标准，如路由协议、安全标准、接入标准和网络管理平台等才能保证实现网络统一，并确保可扩展性；遵循网络分层的原则：在网络构建中，从整体上可以将网络划分为核心层、汇聚层、接入层三个层次，各负其责。

### 3 商行光纤网络具体设计

#### 3.1 层次化网络结构设计

为减少网络中各部分的相关性，便于网络的实施及管理。在网络构建中，从整体个将网络划分为核心层、分布层、接入层。核心层负责高效传输、交换转发及路由分发；分布层负责将各将各种业务集中起来，通过高速接口将数据输送到核心层；接入层设备提供各种标准接口将数据接入到网络中，完成基本的业务系统之间的隔离和安全性控制、认证管理等功能。根据层次化网络设计思想的原则及商行网络系统实际需求及VLAN—VPN接入的特点，我们将商行数据网络中心的局域网与广域网核心层与汇聚层合二为一。

#### 3.2 商行网络的具体网络拓扑结构

整个网络由总行数据中心、各营业网点与离行式的ATM点三个部分组成。如图1所示。

##### 3.2.1 总行网络数据中心网络设计

商行网络中心位于主机房内，采用先进行1000M光纤技术，建设成一个高速交换网络，提高业务处理能力。在总行网络中心新增两台核心交换机catalyst 4507R，用作中心内部网络核心交换机及路由，为各接入层交换机、服务器群提供汇聚和数据交换；因为采用VLAN—VPN的接入方式为RJ45接口，因此可直接接入核心交换机，来完成VLAN—VPN广域网核心接入及路由处理。对内部网络VLAN间路由及访问控制，也交由4507R强大的ACL与路上交换能务来完成。对于业务网与OA等内部办公网间的

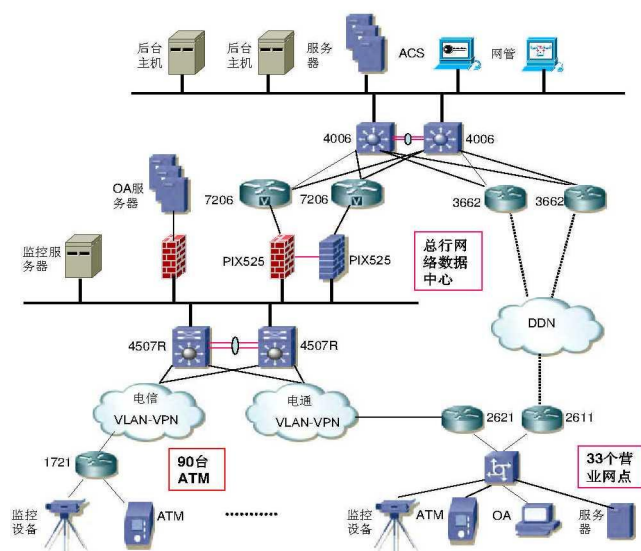


图1 商行具体网络拓扑结构

隔离传输，则由新增的两台Pix防火墙来完成，同时两台防火墙成双机热备系统保障业务数据的可靠传输。在总行中心可配置支持TACACS+、RADIUS服务器来实现认证，或采用ACS认证，同时采用802.1X认证，实现网络安全访问。核心交换机之间采用以太网通道技术，可提供更高的连接带宽。两台核心交换机之间互为备份，分担负载，结合Spanning Tree技术和HSRP技术，任何一台核心交换机发生故障，网络可以在很短的时间内恢复正常。核心交换机上配置有三层交换，提高VLAN间的路由和网络安全控制。

商行中心出于业务数据与其它数据的混合传输安全性考虑及业务数的安全隔离，我们配置了两台pix防火墙，构成双机热备系统，为业务网提供了安全保障。

对于业务数据在VLAN—VPN光纤公共网上传输，如果不进行加密，则业务数据很容易被侦听截获，因此考虑到数据传输的安全性，新增两台cisco 7206VXR来实现核心端VPN接入与数据加密。由于数据是严格加密的，在公网上即使和其数据混杂或者被侦听和截获，也很难被破解和修改，能充分保证数据传输的可靠性、完整性和安全性。具体采用DMVPN技术来实现与各营业网点及离行式ATM点的接入。同时实现VLAN—VPN光纤网传输链路路与DDN线路之间的自动路由切换，进一步提高网络可靠性。

##### 3.2.2 分支营业点网络设计

各营业网点内部网由新增的catalyst 2950交换机来完成VLAN的划分与隔离、三层通过原有的cisco 2611与新增的光纤网接入路由器cisco 2611XM 实现路由及广域网采用VLAN—VPN以及原有的DDN线路实现数据传输功能，光纤和DDN线路互为备份。DDN为业务数据传输的主线路。

##### 3.2.3 离行式ATM点与中心网络互联设计

对于离行式ATM点接入，由于仅有ATM机及监控设备数据传输，因此选用一台cisco 1721路由器通过VLAN—VPN接入方式与中心互联。因为业务数据在VLAN—VPN

公用网上进行传输,为了保障数据传输的可靠性及监控数据分离,我们对业务数据采用了IPSEC加密传输。这样就可以保障业务数据在网络上的安全可靠传输;对于监控数据则按常规方式传输,减轻了路由器的处理负担。

#### 4 全网网络安全设计

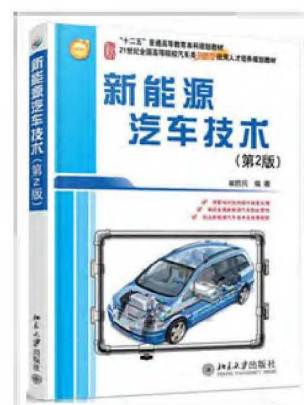
考虑银行业务的特点,网络中的业务数据传输必须要做到安全可靠。安全不仅仅是一个技术问题,同是也是一个管理的问题。但在这里,我主要从技术角度来说明如何确保网络安全。在网络设计中,网络安全管理主要包括以下几个方面:(1)在网管平台、网管软件控制下通过SNMP、RMON协议,实现有关的安全管理;(2)维护并设别被管理设备的运行,防止非法设备接入,防止设备之间的非法操作。网络设备登录采用统一的认证、授权、记帐,采用cisco ACS对网络设备进行统一认证,提高系统安全性。ACS也可以提供802.1x认证服务;(3)实时监测设备运行,异常时报警;(4)对设备设置安全级别,防止非授权修改,配置遭破坏可自动修改;(5)维护网络拓扑的安全,确保交换、路由、VPN网络的正常运行;(6)数据加密传输采用Ipsec VPN、DMVPN技术实现数据的安全传输;(7)审计、分析网络安全事件日志,形成安全决策报告;(8)实现网络风险的集中管理,进行入侵检测、漏洞扫描的管理。(9)网络隔离技术、防火墙技术、VLAN访问控制实现不同部门或不同业务数据的隔离。

#### 5 结束语

通过对商行网络重新规划设计与改造,该商行的网络的可靠性、安全性、稳定性、可用性、扩展性等方面都有了明显的提高,使得网络系统具有优异的性能,为将来商行各种基于数据、语音、视频业务的广泛应用打下坚实的基础。但同时在QOS方面还有待进一步优化,以便于将来部署如VOIP等相关的应用。

#### 参考文献

- [1] Jeff Doyle, Jennifer Carroll. TCP/IP路由技术(第一卷)(第二版)[M]人民邮电出版社,2007.
- [2] Faraz Shamim. IP路由协议疑难解析[M]. 人民邮电出版社,2008.
- [3] 王立新. IP sec与NAT如何共存[J]. 全国网络与信息安全技术研讨会,2004.
- [4] 任云花. OSPF 路由协议的安全性分析[J]. 科技情报开发与经济,2007.
- [5] Wei Luo等. 第二层VPN体系结构[M]. 人民邮电出版社,2006.
- [6] Yusuf Bhajji. 网络安全技术与解决方案(修订版)[M]. 人民邮电出版社,2010.



新能源汽车技术(第2版)

作者:崔胜民 编  
出版社:北京大学出版社  
出版时间:2014-02-01  
ISBN: 9787301237007  
所属分类:  
图书 > 工业技术 > 汽车与车辆

本书对第1版做了适当的调整,使之更加科学合理,对这几年出台的新标准、政策等进行更新、介绍,使内容更新,书中还收录了作者近几年对新能源汽车技术的研究成果及国内外相关研究成果,利于学生更好地了解现在新能源汽车的先进技术。

本书全面系统地论述了新能源汽车技术,阐述了新能源汽车的类型,发展新能源汽车的必要性和新能源汽车发展现状及趋势;重点介绍了电动汽车用动力电池、电动汽车用电动机、纯电动汽车、混合动力电动汽车和燃料电池电动汽车的结构、原理及设计方法等;对天然气汽车、液化石油气汽车、甲醇燃料汽车、乙醇燃料汽车、二甲醚燃料汽车、氢燃料汽车和太阳能汽车的特点、发展现状及趋势也进行了介绍。书中内容既有在新能源汽车上已经广泛应用的成熟技术,也有最新发展的一些高新技术。

崔胜民,哈尔滨工业大学汽车学院教授,山东省新能源汽车首席专家。