学校编码：10384　　分类号_____密级_____
学号：X2011230149　　UDC _____

厦门大学

工 程 硕 士 学 位 论 文

新疆网通 DCN 网络安全的实现与优化

Realization and Optimization of Xinjiang Netcom DCN Network Security

胡金华

指 导 教 师：夏侯建兵副教授

专 业 名 称：软 件 工 程

论文提交日期：2013 年 3 月

论文答辩日期：2013 年 5 月

学位授予日期：2013 年 月

指 导 教 师：_____

答辩委员会主席：_____

2013 年 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　√　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

新疆网通 DCN（Data Communication Network）网络为其各类支撑系统提供专用的数据通信，DCN 承载了运营商各专业网的网管系统（OSS），为其提供了统一的业务传送平台。此外，DCN 还承担了新疆网通的综合业务管理系统（BSS）和管理支撑系统（MSS）。作为运营商日常运作的基础，其重要程度不言而喻。

本论文针对新疆网通局域网络存在的问题,结合具体网络优化技术，以分析归纳的方式给出相适应的优化分析方法。局域网络优化是一个长期的过程,它贯穿于网络发展的全过程。只有不断提高网络的性能,才能更好的发挥局域网络的潜力、提高工作的效率、保障网络的安全,达到最佳的运行效果。

本文从局域网络现状入手，对网络结构、VLAN 技术、防火墙技术进行了论述。星形拓扑结构由于每个节点通过点到点通信线路与中心节点连接，易于进行网络扩展、故障诊断。由于各节点是独立的，增加或减少节点也不需要中断网络，故障诊断时可以中对心节点及其连接线路逐一地隔离开来进行故障检测和定位。通过VLAN 的划分可以限制局域网内广播，减少广播风暴在局域网内的传播，增强局域网的安全性，提高网络之间连接的灵活性。防火墙能使机构内部网络的安全性增强,能加强网络之间相互访问的控制,能防止和避免外部用户非法使用内部网络的资源,能保护内部网络的设备不被恶意破坏,能防止内部网络的重要数据信息不被窃取。另外,防火墙系统还可以限制某些外部网络可以访问内部的资源和服务，哪些内部的资源和服务可以被外部网络访问,以及哪些外部资源和服务在某个特定时间内可能被内部网络访问。

关键词：数据通信网；网络安全；优化；

Abstract

DCN(Data Communication Network) provides dedicated data communication for various supporting systems of Xinjiang China Netcom and a unified transmission platform by carrying on OSS of various professional networks. In addition, the DCN shall also support BSS and MSS of Xinjiang China Netcom. Therefore, its importance is self-evident as the basis for the daily operation of the carrier.

The dissertation comes up with optimized ways suitable to tele-communications enterprise networks with analysis and induction based on current security problems of tele-communications local networks and detailed network optimization technique. The optimization of security of local networks is a long-run process that goes through the whole development of networks. Only when the performance of networks is improved, can the potential of the intranet be played in full length, work efficiency be increased and security of networks be ensured to gain the best effects.

The dissertation discusses the network structure, VLAN technology, firewall technology in terms of the internal network. Star topology which is combined with the center point through point to point communication lines will be easy to carry out network expansion, fault diagnosis. Since each node is independent, increasing or decreasing the number of nodes do not need to interrupt the network and the right center point and its connecting node can be isolated from the network to be used for the circuit fault detection and location one by one. VLAN can be restricted through the division of radio LAN and then reduce the broadcast storm in the local area network communication, enhance security of the local area network, improve the flexibility of network connections .Firewall enables organizations to enhance the security of internal network, also can strengthen the access control of the network and then prevent and avoid external users to visit internal network resources illegally. protect the equipment of the internal network from maliciously damaging, prevent the Important data of the internal network from being stolen. In addition, the firewall system can also limit certain external network to access the internal resources and services, can limit some internal resources and services which can be access by an

external network and some external resources and services which may be accessed by the internal network access.

Keywords: Data Communication Network; Network Security; Optimization;

目录

Contents

第一章 绪论

作为新疆网通的一名从业员工，在工作中时时要用到DCN网络，作为该网络承载相关业务管理系统的使用和应用需求提出意见建议者，从安全的实现和优化方面对该网络进行浅析和探讨。

1.1 研究背景与意义

新疆网通DCN（Data Communication Network）网是为其各类支撑系统提供专用的数据通信的网络，承载了运营商各专业网的网管系统（OSS），为新疆网通提供了统一的业务传送平台。此外，DCN还承担了新疆网通的综合业务管理系统（BSS）和管理支撑系统（MSS）。作为运营商日常运作的基础，其重要程度不言而喻。

根据中国网通管理信息系统部指导意见，中国网通DCN网络建设目标是：建成一个覆盖全国、技术先进、功能齐全的、为公司所有信息化系统提供统一网络承载、统一安全策略、高质高效、可控可管、易于维护的多业务网络平台，满足端到端的业务承载和服务质量需要，保障企业信息可靠、通畅、安全的传送，促进数据共享和资源共享，实现投资效益和管理效益的最大化。

目前原新疆网通DCN网是2004年建设，共承载了ERP、计费、OA、视频会议等9种业务，各业务系统的服务器位于区公司或集团层面。由于原新疆网通的业务量以及整体规模相对较小，该网络配置的设备档次低，已经无法满足日益发展的业务需求。

而原新疆网通没有统一的网络承载平台，其BSS、MSS等核心业务分为多张业务网分别承载在ATM上，其设备陈旧且档次太低，ATM承载也不符合IP化长远趋势，无法满足后续庞大的业务需求。

基于目前业务发展情况，完善网络结构、扩充网络带宽、优化网络的可靠性和安全性已经成为迫在眉睫的需求，而原网络远无法达到需求，因而新疆网通急需新建一张统一完善的DCN网络来对今后不断发展的业务做综合运营管理。

1.2 网络安全的实现和优化的重要性

互联网的迅速普及，局域网应用已成为企业发展中必不可少的一部分。然而，在感受网络所带来的便利的同时，也面临着各种各样的进攻和威胁：机密泄漏、

数据丢失、网络滥用、身份冒用、非法入侵……目前有些企业建立了相应的局域网络安全系统，并制定了相应的网络安全使用制度，但在实际使用中，由于用户对操作系统安全使用策略的配置及各种技术选项意义不明确，各种安全工具得不到正确的使用，系统漏洞、违规软件、病毒、恶意代码入侵等现象层出不穷，导致用户计算机操作系统达不到等级标准要求的安全等级[1]。

目前调查数据表明，我国有 63.6%的企业用户处于“高度风险”级别，每年因网络泄密导致的经济损失高达上百亿。虽然大多数企业都非常重视局域网网安全管理问题，网络安防投入也不断增加，但是局域网安全问题却仍然严峻。在国家出台的《信息安全等级保护管理办法》中，就明确指出了信息安全等级保护的重点在于内网安全措施的建设和落实。事实表明，有效保护企业内部资源和网络的安全，需要建立全面的网络安全体系[2]。

1.3 系统的特点

新疆网通的 DCN 网络和企业的 VPN 网络的需求类似，需要在保证网络的可靠性、安全性和服务质量的基础上，实现部门与业务的隔离和受控互访。本方案的设计特点概括如下：

1、全面采用 MPLS VPN 技术：构建虚拟专网，实现部门和业务的隔离以及受控互访，并采用分层 PE 技术将 MPLS VPN 扩展到分支机构网络；

2、高可靠性：采用电信级设备，通过合理的网络设计，提高网络可靠性，最大限度地支持系统的正常运行；

3、可扩展性：根据未来网络规模和业务模式的变化，网络可以平滑地扩充和升级，最大程度地减少对网络结构及设备的调整，保护投资；

4、可管理性：对网络实行集中监测、分权管理，简化运营管理；

5、开放性：采用开发的技术和国际标准，如路由协议、安全标准、接入标准和网络管理平台，便于多厂家设备混合组网、互连互通。

1.4 论文的结构安排

第一章,阐述 DCN 网对通信运营企业的主要意义，对选题的背景、意义和主要的研究内容进行说明，目前国内外同类系统的情况，安全性方面防范措施、新疆网通 DCN 网络设计特点进行了介绍。

第二章,介绍分析了新疆网通原 DCN 网络情况和问题进行分析。

第三章,重点介绍了新疆网通 DCN 网络根据目前业务和发展情况，高可靠、多业务承载的建设原则方案，设备的选型和具体配置。

第四章，新疆网通 DCN 网络利用 MPLS VPN 技术实现 DCN 网的三层 VPN、实现部门管理和部门间的受控互访。使用 BGP 的 MPLS VPN 是目前应用较为成熟的一种 MPLS VPN 技术，目前各主流厂商互通性较好，商用实例较多。

第五章，对网络安全方案采用内网安全+外网安全方式进行详细说明。

第六章，介绍新疆网通 DCN 网络优化改造工程的 Qos 策略，解决网络延迟和阻塞等问题。QoS 方案提供了多种方案和手段，采用 DiffServ 模型对关键业务子系统服务质量的保证。

第七章,对华为公司 Quidview 网管软件采取分级分权全网管理进行了描述。以及 Quidview 网管性能和 MPLS VPN 业务管理解决方案。

第八章，对本论文描述工程安全方面进行总结和展望。

第二章 原 DCN 网络情况和问题分析

新疆网通作为电信南北拆分后新进入新疆的电信运营企业，经营基础电信业务和电信增值业务，即固话、宽带、数据等业务，组建新疆网通 DCN 网，为其各类支撑系统提供专用的数据通信的网络，共承载了 ERP、计费、OA、视频会议等 9 种业务，没有统一的网络承载平台，分为多张业务网分别承载在 ATM 上，有：BSS 网络、MSS 网络、视讯网、网管、客服网络等，受创业初期人员、业务量以及整体规模相对较小，投资限制，初期建设的 DCN 网络配置的设备档次低，随着业务发展和联通融合，网络已不适应目前的业务和管理需求。新疆网通急需一张统一完善的 DCN 网络来综合运营管理，因此完善网络结构、扩充网络带宽、优化网络的可靠性和安全性已经成为迫在眉睫的需求，只有一张支撑能力强的 DCN 网络才能适应日益增长的业务发展需求，才能支撑电信级的全业务运营，才能带来更多的利润。

2.1 新疆网通原 DCN 网络情况

原新疆网通 DCN 省网以乌鲁木齐、奎屯、库尔勒为核心，乌鲁木齐部署 2 台 P/PE 设备(GER)，奎屯、库尔勒分别使用一台 P 设备(GER)双上行到乌鲁木齐的两台核心，分别接入附近的地市，每个地市有一台 GER 作为地市核心，接入业务，业务通过接入路由器 GAR 接入。

新疆网通原 DCN 网络组网拓扑如图 2-1 所示。