证券数据中心网络系统①

范 君 解圣霞 (南通纺织职业技术学院 江苏 南通 226001)

摘 要: 数据中心作为证券等金融机构关键数据平台，其网络系统地位极为重要。针对某证券公司在实施数据中心建设过程，根据需求提出了网络中心设计原则和建设目标，阐述了其数据中心网络系统的核心业务网络、交易与办公系统网络、广域网等不同网络系统的设计方案。新的网络系统设计经运行表明，满足了系统业务需求，实现了建设目标。

关键词: 数据中心；网络系统；系统设计；负载均衡；广域网

Securities Data Center Network

FAN Jun, XIE Sheng-Xia

(Nantong Textile Vocational College, Nantong 226001, China)

Abstract: Data center is the critical data platform to the system securities and other financial institutions. The status of its network system is extremely important. During a securities firm in the implementation of data center construction process, on the basis of need a network centric design principles and construction goals, this paper describes its data center network core business network, trading and office system network and wide area networks systems design. The operation of the new network system design shows that the system meets the business needs of the system and achieves the development goals.

Keywords: data center; Network system; system design; load balancing; wide area network

为适应业务不断增长的规模和新的应用需求，某证券公司于 2009 年对其华南数据中心网络实施升级改造建设。作为公司的中心节点，打造一个安全、高效、高可靠性的全新的数据中心网络系统是此次建设规划的核心。本文从项目实施的角度，重点介绍网络系统的整体设计与技术实施。

1 系统建设的总体目标

该证券公司的网络系统建设的总体目标是：利用先进实用的网络技术和网络设备，建设一个满足新业务需求的中心网络节点，实现和其他中心节点数据互访、备份，并满足所在地的营业厅对中心节点证券交易系统的实时访问，并提供稳定、高效的网络接口实现本地办公网、分支机构对数据中心安全的访问。同时网络应当具有高安全性、高稳定性，支持高并发、大流量的业务，并对有实时性需求较高的视频、语音等业务保证服务质量，能够满足不断发展的需求。

2 系统业务需求和设计原则

2.1 基本业务需求

根据该证券公司网络系统建设目标和远景规划，网络系统应具备以下的处理能力：持续业务交易处理能力达到 1 万笔/秒，全天可处理超过 4000 万笔的成交记录，并且网络架构能够满足今后几年内业务增长的需求，而且能够支持本省的各个营业厅、分支机构及其他省中心交易平台对该网络系统平台的访问。

2.2 系统设计原则

(1) 可用性与先进性

数据中心的主干网络要求能够支持高带宽和大吞吐量，对于语音和视频数据流量要有实时性和质量保证，在业务流量高峰期间网络中不存在任何瓶颈，并避免任何可能的流量拥塞和数据包丢失的情况发生[1]。

① 收稿时间:2010-04-06;收到修改稿时间:2010-04-26

网络设备对并发连接数、会话处理能力要有足够的支持。

在满足证券业务、应用系统业务的数据传输需求前提下，网络的设计要体现出其先进性，采用新技术和新设备，力求使网络既能满足当前需要，又能适应未来业务发展的需求。

(2) 可靠性与安全性

证券网络要求高可靠性、高稳定性，要求网络设备具备提供 7*24 的不间断服务能力，因此网络设计需要提供足够的冗余设计和必要的备份，以防范任何可能的单点故障造成网络功能的停歇。冗余设计包括电源冗余、链路冗余、设备冗余、路由冗余，对于关键设备、线路要求能够做到实时备份和故障自动切换[2]，同时对于数据采用必要的备份以确保数据完整性。

网络安全性在整个系统中至关重要，一个安全的网络应该有必要的技术和安全措施，控制网络中数据信息使之具备高度的安全性和保密性，能够阻止非法入侵和信息泄露。

(3) 标准性与可扩展性

网络系统的设备、技术在具备先进性的同时，需要考虑到标准性。通过采用符合国际和国家标准的网络设备、主机设备、存储设备、数据库系统、中间件系统及协议，按照国际和国家统一的规范和原则，兼容不同厂家的软硬件产品。

考虑到证券业务的目前及远景规划，具备标准性的证券网络系统应当在未来业务发展和变化中，能够平滑扩展和升级，以期最大化减少对现有网络基础架构的调整变动[3]。

(4) 可管理性与可维护性

网络系统应该便于管理、配置和调整。网络系统监控管理应该和主机、存储等其他业务系统的监控管理有效融合，便于管理维护人员对系统中的软硬件各个部分进行监控，了解系统运行状态、资源配置和使用状况，以控制系统运行并对故障在第一时间内完成处理。

3 核心业务网络设计

核心业务网络作为证券集中交易网络子系统(含证券实时交易系统、存储备份系统)、应用业务系统、前台交易网络子系统、办公网络子系统等各个系统提供网络基础结构并承载上述各个子系统的数据业务，核心业务网络在体系结构上采用了核心层、汇聚层、接入层的三层结构。

3.1 核心区网络设计与实现

该区域的核心层采用两台 7609-S 运营级模块化交换路由器，下行通过多台 BIG IP 负载均衡器 LTM VIPRION 及多台 ASA5540 防火墙接入到汇聚层设备。每台 7609-S 路由器上配置了多块 WS-X6704-10GE 线性卡模块。同时通过配置了 WS-SVC-IDS2-BUN-K9 服务模块，实现对进入 7609 内部的数据进行 IPS 防护，实现 IPS 入侵检测防范功能，对于内网的数据流实时监控防止对内网服务器主机系统可能的入侵，借助 7609 的高速引擎及背板总线快速数据传输功能实现了高速数据防护。

汇聚层使用了四台 6513 运营级模块化交换机，每两台 6513 作为一组，两组 6513 分别承担系统核心业务。每对 6513 交换机上借助 WS-X6704-10GE 线性卡模块的 10GE 的万兆端口实现核心交换机 10G 数据承载能力。6513 对下联各个业务子系统划分 VLAN 的三层网关地址配置于每组的核心交换机上，通过对配置 HSRP 网关地址使得每组的两台交换机互为热备。在一组内部的两台 6513 之间各自提供 4 个 10 GE 端口，使用端口聚合技术 EtherChannel 捆绑为一条 40G 的逻辑链路，从而实现达到增加带宽,提供冗余的目标，并且在该链路上启用 Trunk 链路，封装 dot1q 允许不同的 VLAN 数据流通过。

接入层设备使用的是 Nexus 5020 交换机，该交换机连接 6513 上联端口及互联端口均用 10G 端口并配置 EtherChannel 实现数据传输的高可靠性与高效性。Nexus 5020 交换机的下联 IBM 刀片式服务器群及 IBM System P595 小型机。Nexus 5020 交换机除上联至 6513 外，还将上联至存储区光纤通道交换机 MDS9506，借助 Nexus 5020 交换机与 MDS9506 交换机之间的光纤通道连接，实现数据区与存储区的互联。这种设计通过将传统数据中心的以太网络线路、光纤通道线路进行了有效的融合，极大减少了访问层中的物理线路和交换机的数量并便于今后的网络扩展。核心网络整体的体系结构拓扑图如图 1 所示。

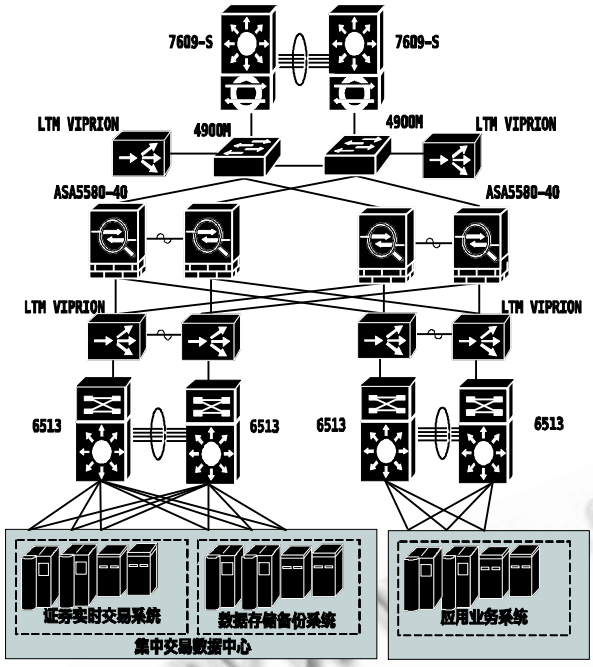

图 1 数据中心核心网络体拓扑图

3.2 流量负载均衡设计与实现

集中交易网络系统中的行情服务器和交易服务器上的业务流量，需要保证在任何时候行都不会中断。对于各种可能的突发情形都需要有着实时响应处理能力以保障上述业务流量的高可用性，同时对进入防火墙的流量也需要进行有效的负载和分流。

为实现上述目标，在核心网络中部署了三对 F5 LTM VIPRION 四层交换机用于服务器及防火墙的流量负载均衡。其中第一对 LTM 部署在 7609-S 和 ASA5580-40 之间用于实现防火墙的负载均衡。其他两对 LTM 部署在 6513 上，支持防火墙负载均衡同时用于实现服务器的负载均衡 [4]。F5 LTM VIPRION 采用刀片式架构支持四个刀片板卡，每个刀片板卡能够支持 9G 四层或七层吞吐量，七层处理能力达到 80 万会话数/秒，这个处理能力完全满足对于目前及将来的业务需求。对于本系统除了系统之间需要进行数据流量的负载均衡外，还针对证券业务中涉及到的行情信息查询等 Web 流量较大的信息进行必要的 Web 加速，以提升链路访问的效率和带宽，同时对 SSL 业务实现加速，将 SSL 的处理压力转移到 VIPRION 上以降低服务器的 SSL 负载。

3.2.1 防火墙的负载均衡实现

防火墙负载均衡采用 F5 常见的三明治结构，位于 6513 上行线路上的四台 ASA5580-40 分成两组，每组内部的两台防火墙工作于 Active/Standby 模式[5]，通过将 LTM VIPRION 置于 ASA5580-40 防火墙的上下两侧，负载均衡器对防火墙构中的用户会话上下行数据流进行监控，维持会话的完整性和合法性。

防火墙上下层的两台 LTM VIPRION 均为 Active/Standby 模式工作，下面分析均以上层的两台 LTM 为例。每台 LTM 上行使用双 10G 网线捆绑为 F5 的 Trunk(即 Link Aggregation)连至 4900M 交换机，这样既保证了线路的可靠性又提高了上行链路的数据传输流量，这两根线路端口划分到 external vlan；下行则使用两根 10G 网线分别连接不同组内的两台 ASA5580 防火墙，端口划分到 internal vlan。每对 LTM VIPRION 之间通过 HA 线路互联检测链路和设备的状况，一旦主设备发生故障，就进行毫秒级主备设备切换。在 LTM VIPRION 上创建地址池，两台防火墙的 outside 端口地址作为地址池成员。当来自营业厅、办公网等区域的访问数据从 7609-S 转发到 LTM VIPRION 时， F5 设备自行检查数据流量，根据目标地址信息和负载均衡算法，把数据包分发到两组防火墙中的一组处于 Active 的设备 outside 端口上[6]。

3.2.2 服务器的负载均衡实现

核心网络体系结构中的下层每对 F5 LTM VIPRION 在承担防火墙负载均衡工作的同时，也承担了服务器负载均衡的工作，和上层的设备类似，也工作在 Active/Standby 模式工作，根据后台服务器类型的不同分别定义服务器群组创建不同地址池，VLAN 的划分则和前面类似。

对于所有的对外提供服务的服务器，均可以在 LTM 上配置 Virtual Server 实现负载均衡，同时 LTM 可持续检查服务器的健康状态，一旦发现故障服务器，则不再将流量转发于该设备。LTM 连续地对目标服务器进行 L4 到 L7 合理性检查，当用户通过 VIP 请求目标服务器服务时，LTM 根据目标服务器之间性能和网络健康情况，选择性能最佳的服务器响应用户的请求。

4　交易与办公网络系统设计与实现

办公网络系统和交易前台网络系统因楼层分布、接入点较多，在接入层之前使用了两台 Cisco 的 4507 交换机作为汇聚层设备，该汇聚设备使用单上行线路，每对设备间设置 HSRP 互为热备，在设备上 HSRP 浮动地址作为各楼层的办公区域的终结网关，4507 和 7609-S 之间通过静态路由转发数据。接入层的 3750E 交换机通过两个 10GE 线路分别接入两台 4507 交换机。

证券公司的总部办公网中绝大多数终端用户都具备了便携式计算机，且每层办公大楼有多个大小不等的会议室、培训室、报告厅、多功能厅，故在这些公共场所为终端用户提供安全的无线接入是必要的。无线接入 AP 使用了 Cisco Aironet 1240AG，采用 IEEE 802.11a 及 IEEE 802.11g 相结合的技术实现无线网络覆盖，其 100M 上行线路接入 3750 交换机或 2100 无线局域网控制器。为更好管理无线接入和无线网络的安全性，在无线网络接入中使用了多台思科 2100 无线局域网控制器 SWLC，为网络管理员提供了必要的安全性、可靠性，如安全策略、入侵防御、RF 管理、QoS 和移动性等，以上的特性可以由网络管理员根据业务发展变化进行调整和部署。交易与办公系统网络拓扑图如图 2 所示。

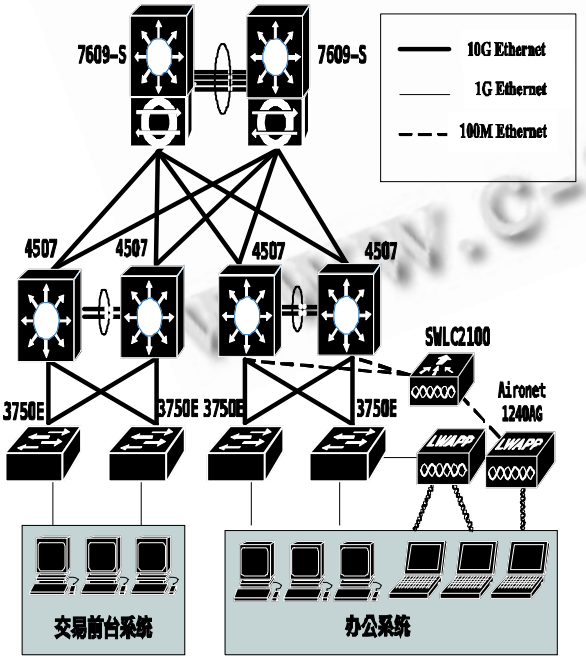

图 2　交易与办公系统网络拓扑图

5　广域网设计与实现

在广域网设计部分中，根据该证券公司的业务发展需求，需要分别为外省的其他中心、本省分支机构、省内营业厅提供必要的访问链路接口，对于上述三种不同的访问需求在广域网设计与实现中需要区别对待。为提供较大的带宽和较高的通信质量，该网络系统使用 Cisco ASR1000 系列路由器作为网络边缘路由器承载数据转发。

5.1 广域网设计

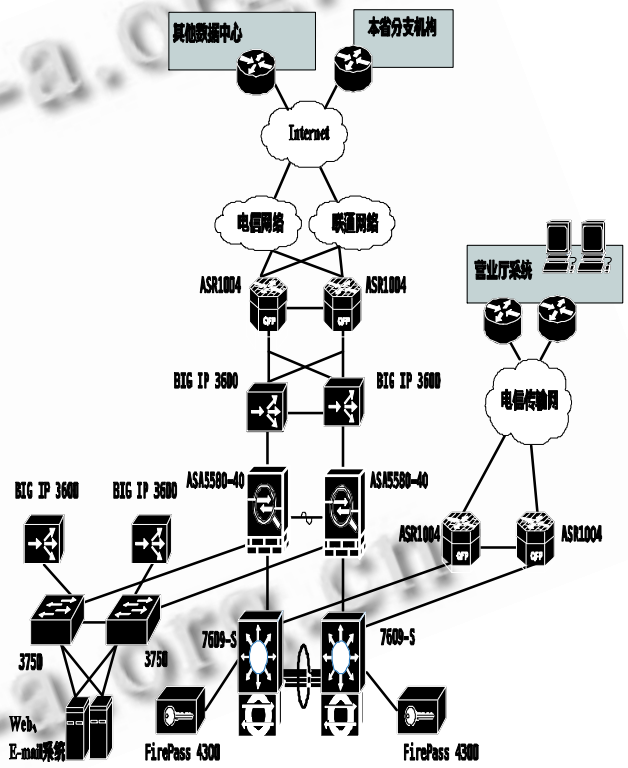

图 3　广域网体系结构整体拓扑图

对于和省外的数据中心互联需要，在 Cisco ASR1004 路由器上使用了多条专线接入电信网络，以满足证券网络内部通过互联网访问其他中心的需求。考虑到证券系统对实时性、线路不可中断的高需求，在实现电信广域网接入的同时也实现了到联通(原网通)广域网的接入。以电信接入的广域网线路为例，两台 Cisco ASR1004 路由器将分别接入到电信的 163 网络及电信 CN2 的 MPLS VPN 网络，163 网络的链路用于提供普通互联网访问，MPLS VPNL 链路则将路

由器作为 CE 设备和电信端的 PE 设备相连，以实现各个中心之间的安全互访。

普通用户、集团用户通过互联网线路访问位于 DMZ 区的 Web 系统，并且允许集团用户访问 E-mail 系统。另外，本省的分支机构的访问则通过互联网线路，在进入 ASR1004 前需要通过 SSL VPN 的方式访问内网的服务器资源。

为满足营业厅访问集中交易网络系统的应用要求，当地的营业厅分支机构通过 100M 的线路接入电信传输网络访问 ASR1004 路由器。广域网体系结构整体拓扑图如图 3 所示。

5.2 广域网链路负载均衡与 SSL VPN 接入设计

本省的分支机构访问数据中心需要网络提供一个安全可靠的访问方式，使得机构内部员工可以从互联网直接访问数据中心的业务信息，在系统设计中，借助了 F5 FirePass 4300 设备 VPN 功能，以 SSL 为传输协议，实现了 2000 个并发用户访问的连接。同时在边缘路由器下联各接入一台 F5 BIG IP 3600，在电信或联通任一链路故障时能够实现将网络数据传输自动切换到另一条链路。和前面数据中心核心网络 LTM 功能不同的是，此处的 F5 设备具备链路控制模块 LC，借助 LC 模块功能成功实现链路负载均衡。

6 结束语

本文描述了证券公司省数据中心网络的设计工作，具体涵盖了该中心的核心区网络系统、交易与办公网络系统、广域网系统的设计，并阐述了网络设计中涉及的负载均衡实现。新的数据中心强有力支持了该省的业务数据，为提升证券公司整体业务处理能力和适应新应用的需求奠定了良好的基础，并为其他中心改造升级提供了成功案例。

参考文献

1 Oppenheimer P. 自顶向下网络设计.第二版.北京:人民邮电出版社, 2007:27－37.

2 Bhaiji Y. 网络安全技术与解决方案.北京:人民邮电出版社, 2009:141－144.

3 Teare D, Paquet C. 园区网络设计.北京:人民邮电出版社, 2007:10－14.

4 F5. Configuration Guide for Local Traffic Management v9. 2005:33－52.

5 Santos O, Frahim J. Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance 2nd ed. Indianapolis: Cisco Press, 2005:548－555.

6 Deal R. Cisco ASA Configuration. Columbus: McGraw-Hill Os