中国联通集团 IDC 流量监测项目
成功案例

东华软件股份公司

2013 年 2 月

1. 项目概述

2008 年 10 月，北京东华合创科技有限公司（现更名为东华软件股份公司）中标“2008 年中国联通 IDC 流量监测和资源管理平台建设工程（流量分析系统）”项目。

中国联通集团（原中国联通集团）根据 IDC 业务发展的需求，为了提升 IDC 业务的运维水平，优化 IDC 业务的服务质量，加强 IDC 业务的竞争力，打造一个可运营、可管理的宽带精品网络，在网络的质量、业务的种类、网络的可靠性和安全性等方面有很好的保障，在业务和服务方面优于其他运营商的网络，能够为高中端客户提供电信级的业务承载，从而树立中国联通的宽带网络品牌，决定启动“2008 年中国联通 IDC 流量监测和资源管理平台建设工程”。东华软件股份公司参与了本工程项目的投标，在与国际知名厂商竞争中脱颖而出，并以其优秀的产品解决方案和卓越的服务体系等优势赢得了合同。

本项目方案采用东华流量分析产品（ForceView FlowAnalyzer）,在北京建设中国联通 IDC 流量监测和资源管理平台全国中心，实现对全网 5 星级及 4 星级 IDC 节点的统一客户信息管理、资源统一调度和管理、流量监测和分析等，加强 IDC 网络的可视性与可控性。

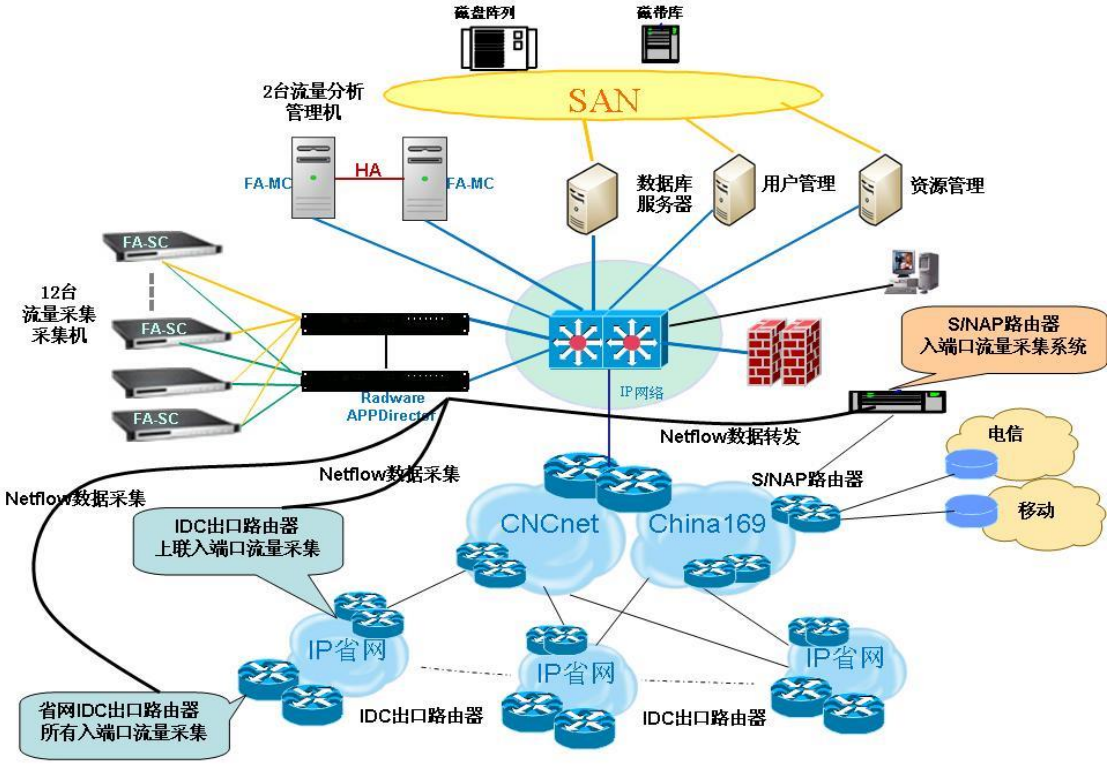
FlowAnalyzer 系统能够支持每秒 8 万个数据流的处理能力，该项目采用 12 台 FA 设备，应用负载均衡方式集中部署，管理涉及本次工程的 22 个省 30 多个 IDC 节点的约 1930G 网络流量，总处理能力为 80 万流/秒。它通过采集 IDC 出口路由器、IP 网骨干路由器、网间互联路由器等 Netflow/BGP/SNMP 信息，进行全网流量关联分析、网内热点的流量分析、热点网站的监测分析、BGP 路由分析、异常流量监测与缓解、内容源流量监测、基线分析、流量实时监控、流量报表展现以及提供大客户增值业务服务等。

中国联通集团运用 ForceView FlowAnalyzer 系统平台，可实现基于 IDC 业务的流量流向和流量成分的分析，分析总体业务发展趋势和客户行为，为网络瓶颈排除和性能优化提供依据；对网络资源的使用情况进行管理，避免因为资源使用过度或使用状况不明所导致的网络服务质量下降；实现性能统计和性能趋势分析，提供灵活的报表功能，提高网络运行维护水平；提供多样的历史资料条件查询和统计分析，便于指导 IDC 的规划和资源优化，为 IDC 业务发展提供数据依据；实现全国 IDC 资源的统一调配。

2. 项目需求建设

本项目的总体功能架构：

此项目部署了 12 台流量采集分析机（FA-SC4050），单台的采集分析能力为 80000flows/sec， 2 台流量集中分析管理设备，系统使用资源平台数据库，建议为 Oracle 数据库，在线保存三年的分析数据约需要空间 8TB。



通过本平台的建设实现了：

网内热点的流向分析

分析各个省 IDC 的热点 SP/CP 的流量流向、监控省间的穿网流量，监控各个省的 IDC 发展状况，避免内部的恶性竞争。同时对不合理的 SP/CP 服务器部署，给出建议和指导意见。

热点网站的监控

监控网通用户访问异网的热点网站，并对其流向分析做出长期监控。

监控省网 IDC 内的资源热点，并对其发展的趋势和流向进行长期的监测分析。通过分析 IDC 出向流量对资源热点进行长期的监测，帮助宽带业务部门对有价值的热点进行品牌的包装，在网通内部统一推广。

要能通过 DNS 和 IDC 的资源信息得出热点的具体栏目和频道。

IDC 异常流量的侦测和缓解

能够实时监测针对 IDC 托管客户，以及网络范围的 Dos/DDos 网络攻击，对攻击的

来源、目的、攻击的类型、攻击的规模、持续的时间、影响的范围进行及时的分析呈现，并支持多种方式告警。

能够对 IDC 托管客户，以及网络范围内的主机，进行出向流量的实时监测分析，及时发现网络 Worm 蠕虫病毒的爆发，对病毒流量的来源、目的、产生的流量规模、持续的时间、影响的范围进行及时的分析呈现，并支持多种方式的告警。

能够对发现的针对 IDC 托管客户、以及网络范围的 Dos/DDos 网络攻击，系统能够通过 BGP 路由牵引的方式在路由器上实现 blackhole 的异常攻击流量丢弃。

流量增值业务的提供

为客户提供独立的登录界面；

为客户提供长期流量监测，并应提供日、周、月、季度、年等多种统计分析报表。

为客户提供实时流量监测。

为客户提供自己网络范围内异常流量的实时监测、分析告警的增值服务。本工程系统应具备此项功能，但本期工程仅在部分节点作试点。

内容源流量监测

可以监控出未列在本管理平台的 IP 地址资源表中的内容源，列出此内容源的 IP 地址及其相关内容、位置和流量流向。

3. 项目收益

东华流量分析系统具有以下功能特点，这些特点一定能够在中国联通 IDC 流量监测项目中得到体现。

1、东华流量分析系统是全网关联的流量分析系统，以电信运营商网络的观点来看全网的流量，并非单个设备或单个端口的角度来对流量进行分析。在本项目中，采用多个监测点采集，集中分析管理，能够将中国网所有的 IDC 流量进行集中分析；

2、东华流量分析系统支持 BGP 路由和 BGP 路由的分析，能够根据 BGP 特点详细精确的分析网络的对外的流量，同时提供对路由的震荡和路由劫持事件的发现；

3、东华流量分析系统能够提供完整的应用分析和应用排名、热点地区分析，帮助运营商掌握运营情况，提升运营管理水平；

4、东华流量分析系统具备详细的 Peer 分析功能，提供强大的过路流量和对外网流量的分析；

5、东华流量分析系统具备强大的用户分析功能，可实现用户和内部网络元素对外部网

络之间、特定 AS 之间，特定过路 AS 和特定网络元素、用户之间、用户应用、用户 Top session 等的流量关联分析功能。更加详细分析大用户的业务需求和流量走向。这项功能将帮助运营人员了解 IDC 业务大用户的使用情况，并可以为大用户提供流量流向分析报告，更好地服务大用户；

6、东华流量分析系统具备真正的实时性的网络分析，提供网络现在的流量分析状况的实时汇报，帮助 IDC 运营人员最及时地掌握 IDC 业务的现在运行情况；

7、东华流量分析系统本身提供长时间的分析数据存贮功能，可提供三年内指定时间段的流量分析功能，结合本项目的磁盘阵列和备份系统，系统可以更长时间的保存分析数据；

8、东华流量分析系统提供统一的管理界面，设备体系结构采用 2 层结构，存在多个采集分析设备的情况下由集中分析管理设备进行统一的管理和配置，并实现数据关联。无须对多个设备实现单独的授权和管理；

9、东华流量分析系统是完全中国知识产权的流量分析产品，系统界面完全使用中文，并提供完整厂商本地化服务，结合本项目，我们将提供深入的二次开发服务，将流量监测与资源管理平台进行深入整合，将两个系统完全融合成一个 IDC 业务的综合管理平台。