华夏银行 HUAXIA BANK

华夏银行总行

案例介绍

东华软件股份公司

http://www.dhcc.com.cn

一、 现状分析

随着华夏银行业务迅速发展和各种基于网络业务应用的部署，特别是总行到一级行、二级行的广域网已经承载了本行各项业务操作数据。然而，伴随着正常应用流量，网络上形形色色的异常流量也随之而来，甚至是看似正常实际异常网络流量大量占用网络设备系统资源（CPU、内存等）和网络带宽资源，使网络产生拥塞，造成网络丢包、时延增大，最终可能造成整个网络瘫痪（例如民生银行网络瘫痪事件）。

由于逐渐实现全行业务大集中，对全行网上业务进行统一融合，以达到统一业务网内关键性业务应用，并强化关键性业务优先的保障目的。全行网络上各种应用越来越多、越来越复杂，而网管人员对这些应用的可监视性、可控性、可预测性的手段却相当有限。华夏银行虽然在 IT 基础设施建设方面已经具备了一个网管中心，负责对全网进行管理。但是在业务精细化监控运维管理方面，目前还存在的主要问题是业务应用的可视性和可控性薄弱。

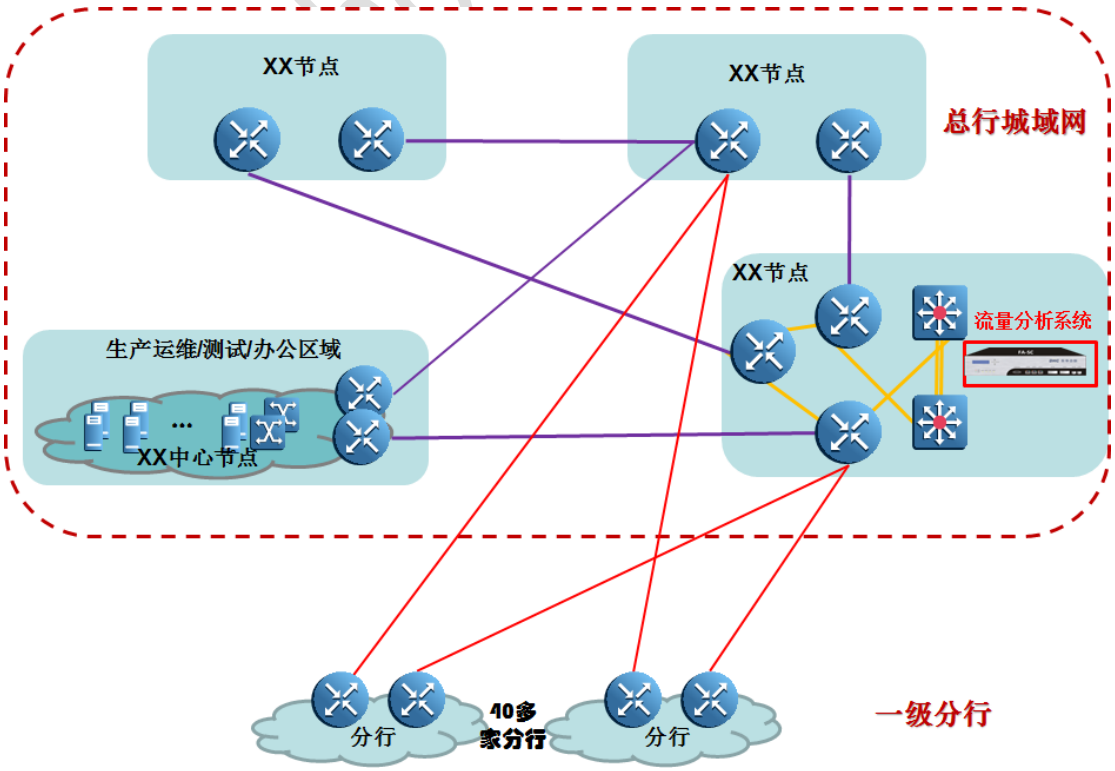
- 网络透明度降低：
  - 网络状况日趋复杂，大量新兴应用涌现
  - 缺乏对全网流量的整体把握
  - 无法实现对网络流量的精细化分析
- 大量未知流量挤占网络资源：
  - 各种网络流量吞噬带宽
  - 非关键应用无法得到管理
  - 异常流量威胁网络安全
- 网络稳定性、安全性下降：
  - 网络拥塞时有发生
  - 关键应用无法得到保障
  - 病毒、网络攻击可能导致网络瘫痪

随着业务的发展和网络数据量的增加，本行业务网络面临带宽资源匮乏的问题。增加带宽虽然能暂时解决燃眉之急，但是会带来网络租用费用的大幅增加，依然是项治标不治本的方法。业务融合系统的高抢线性导致带宽有多大，应用便占用多大，永远保持实时的带宽最大化占用量。造成网络资源严重浪费。

二、 解决方案

鉴于上述网络现状和问题的分析，为了提高华夏银行业务网的运行效率和管理效率，降低企业的 IT 网络投资成本，需要对整个网络的高效运行维护提供一个高可用性的网络平台，使其成为华夏银行业务迅速发展的重要基石。在面对复杂的异构网络环境，需要对网络中各种业务应用所占用的带宽资源有清晰的了解。对当前网络应用情况进行实时、长期的监控，实现网络的透明化管理。通过相应优化策略，对关键性应用给予高带宽、高优先级进行保障，对非关键性应用进行限制，对一些恶意的网络攻击行为进行抵御。优化系统布置以根据业务应用需要对出/入网的流量进行控制，对每种应用占用带宽进行合理分配，从而保障整个网络的稳定运行，缓解网络扩容压力，同时实现网络性能和效率的最大化。

网络部署示意图：



三、 部署收益

部署流量分析系统关键收益：

- **能够帮助维护人员全面深入分析网络流量的分布情况。**

  可以按照应用类别、按照源地址、目的地址、自治域等对网络流量进行分析，了解网络中发生了哪些流量？哪些流量占用大量带宽？哪些用户的延迟和响应速度慢？帮助确保关键业务正常运行。

- **能够帮助维护人员快速发现网络中的异常流量并准确定位异常流量的影响范围、异常流量的来源和目的及其细节特性。**

  异常流量的源 IP 地址、目的 IP 地址、源端口、标端口、网络层协议类型、TOS、输入接口的逻辑接口索引等细节。

- **如果由于遭到 DOS/DDOS 攻击、冲击波、Red Code 等蠕虫病毒攻击引发流量异常时，能够帮助维护人员快速定位是哪台主机引发的。**

  网络蠕虫攻击一般在流量、协议、攻击端口以及攻击行为方面会具有一定的特征。因此，在对这类网络蠕虫攻击进行监测时可以根据其特征进行判断，建立有一套蠕虫攻击特征的分发和收集系统，这种智能化的蠕虫攻击特征检测可以提高已知蠕虫特征的攻击监测准确性，也可以提高监测未知蠕虫攻击的能力。

- **流量异常报警、识别将要发生的网络拥塞**

  通过对网络中一些特定流量的长期监控，网管人员可以了解网络的流量模型和趋势，逐步形成网络流量的基线数据，根据对重要用户、业务、或可能病毒流量的实时监测数据，并对比流量的基线数据，可以识别将要发生的网络拥塞，从而起到预警作用。用户可以自行定义告警模板；并可根据已知的攻击和病毒端口，定义告警列表，这样当监控点的网络流量及持续时间超过阀值，系统即通过相关方式告警。

- **快速定位和解决网络问题；**

  当发现网络流量异常时，能快速判断引发原因，结合流量实时查询、TOPN 排名功能可以定位瞬间异常流量的产生及影响范围、异常流量的来源和目的及其流量的细节特性，从而快速定位和解决故障。

- **优化网络结构，降低网络运行成本，为网络投资升级提供准确的量化依据；**

  通过提供的网络流量的来源、目标；高峰低谷的差异；网络应用等各种数据的比例分布：关键业务、非关键应用和娱乐性应用及关键用户、关键设备的带宽、流量占用分布情况，为带宽资源的重新调整控制提供准确的依据，从而优化网络结构，降低网络运行成本，为网络投资升级提供准确的量化依据。

通过东华流量分析系统，对当前华夏银行网络（总行及下属行）应用情况进行实时、长期的监控，实现网络的透明化管理。优化系统，了解业务应用出/入网的流量状况，从而构建一个**“可监视、可预测”**华夏银行业务网络，保障整个网络的稳定运行，缓解网络扩容压力，同时提升业务运营的效率、降低运营成本。