

企业级应用集成平台研究与应用

朱海虎

(吉林移动业务支撑中心, 长春 130000)

[摘要] 吉林移动是信息化体系建设比较发达的大型企业, 业务运营支撑系统需要与大量外部平台进行交互, 通过企业级应用集成平台建设实现外部接口的统一管理, 提升企业信息化管理水平。

[关键词] 业务支撑系统; 应用集成平台; 通讯总线; 适配器

doi: 10.3969/j.issn.1673-0194.2014.10.029

[中图分类号] F272.7 **[文献标识码]** A **[文章编号]** 1673-0194(2014)10-0043-03

吉林移动是信息化体系建设比较发达的大型企业, 业务运营支撑系统规模庞大, 支撑业务种类多, 需要与大量其他平台进

行交互, 有时作为业务发起方, 向外部平台发起请求交易; 有时作为业务受理方, 处理外部平台交易请求。随着客户数量和业务量增加, 由于未对系统外部接口统一管理, 外部系统的接入对系统压力越来越大, 利用企业级应用集成平台统一规划业务支撑系统

[收稿日期] 2014-03-21

1 威胁园区网数据安全的情景

1.1 计算机操作系统漏洞

任何一个计算机操作系统都有漏洞, 很多人没有及时更新安全补丁的良好习惯, 造成用户电脑或服务器处于危险状态, 同时, 随着越来越多的个人设备投入到办公中, 这些 BYOD 设备管理难度更大, 威胁到在这些系统中数据的安全。

1.2 计算机病毒的传播

随着 U 盘等便携存储设备和网络的扩展, 各种病毒也利用这些通道进入企业网内部, 威胁到个人信息和企业数据安全, 特别是一些木马类病毒, 往往造成的破坏性更大。

1.3 来自内外部的攻击

为了某种目的的内部网络攻击呈现逐渐上升的状态, 在企业中, 篡改人事系统档案和记录, 越权查看公文, 窃取客户隐私、获取企业机密文件等现象越来越多地出现在我们面前。随着网络的发展和知识的传播, 网络攻击的门槛越来越低, 黑客可能只是点点鼠标运行软件的电脑菜鸟, 就完成了攻击行为。

1.4 硬件故障

计算机硬件不能也不可能保证终生无故障, 即使像存储这样的设备也有可能出现硬件故障, 而导致存储的数据全部丢失, 无法找回。而用户个人的设备, 硬件稳定性要更低, 没有合理的备份策略, 一旦出现硬件故障, 损失将不可估量。

1.5 管理权限不清

企业包含不同部门、人员, 这些部门和人员与其对应的数据操作管理权限有很大区别, 但是企业往往把网络管理、数据管理作为纯技术来处理, 对园区网没有一个整体权限设计, 造成数据丢失、窃取和篡改。

2 数据安全策略的制定

2.1 设备保障

企业园区网数据安全主要威胁来自网络, 网络安全设备主要包括在园区网中接入软、硬件网络防火墙、入侵检测与防御系统、防病毒系统、漏洞扫描工具、用户审计等。防火墙是传统网络安全设备, 它可以有效控制园区网与互联网之间的数据传送, 在数据层面上保护内部网络的数据不被外部非授权用户访问以及过滤非法信息。而入侵检测与防御系统, 主要用来帮助处理网络攻击, 提高园区网的安全事件应对能力。防病毒系统能针对病毒特点以硬件或软件的形式处理病毒造成的安全问题。漏洞扫描工具是未雨绸缪, 在未发生安全事故前, 模拟攻击以发现园区

网和各系统中的漏洞并修补。用户审计师对园区网内上网用户行为的规范, 阻止网络中的违规操作, 增强园区网安全性。

2.2 接入认证

园区网全面实施接入用户认证, 从源头上杜绝匿名非法用户窃取数据的可能性, 同时限制接入对象的数据使用权限。

2.3 区域限制

在园区网内划分不同的区域, 可以使用组或交换机的访问控制列表(ACL)、VLAN 等功能, 区分不同用户对数据的访问权限, 降低内部攻击对数据安全的威胁。

2.4 备份恢复机制

建立统一完善的数据备份机制, 对于一个重视数据安全的企业来说非常重要。这个数据备份机制不仅包含企业数据的备份还应包括员工个人数据的备份。无论是选择专用的备份硬件和软件, 都应达到一旦出现故障, 能在最短的时间内, 利用备份的数据恢复到故障之前的状态, 保证数据安全性和完整性。

2.5 数据加密机制

重要数据的加密, 对于一个企业来说太重要了, 合理的数据加密策略, 可以保障企业核心数据的安全, 同时不会出现数据加密和解密时间超出可接受范围的情况, 即使数据出现泄露, 没有相应的解密密钥, 获取方也无法查看数据。

2.6 管理制度

用制度来约束人, 没有完善的信息管理制度, 任何技术层面的策略都是徒劳的, 只有将人的保密意识、操作规范、安全策略置于管理制度下, 才能构成完善的数据安全体系。

3 结束语

保证数据安全是网络管理的重中之重, 网络安全策略是一个随时变化的系统工程。园区网络是不断升级发展的, 要实时关注网络安全面临哪些威胁和攻击, 及时分析、评估新技术所产生的安全风险, 并有针对性地设置新安全策略。

主要参考文献

- [1] 李春青. 高校校园网络安全分析和研究对策[J]. 网络安全技术应用, 2012(9).
- [2] 张军伟. 高校网络安全分析及其对策[J]. 网络安全技术与应用, 2009(10).
- [3] 乔军利. 企业内部计算机网络安全问题与防范[J]. 西铁科技, 2010(1).
- [4] 张庆伟. 校园网安全控制策略探究[J]. 河南农业, 2011(2).

与各平台接口,解决企业信息化管理中遇到的问题变得十分迫切。

1 移动业务支撑系统接口管理现状

业务运营支撑系统在与各平台进行交互时,根据平台提供的接口协议、报文格式、接入方式等内容,对每一个应用平台单独进行接口程序开发工作,外部系统通过各个接口与业务支撑系统进行业务交互,随着业务的增加,接口程序呈现出烟筒状的增长方式,并出现以下问题(如图1)。

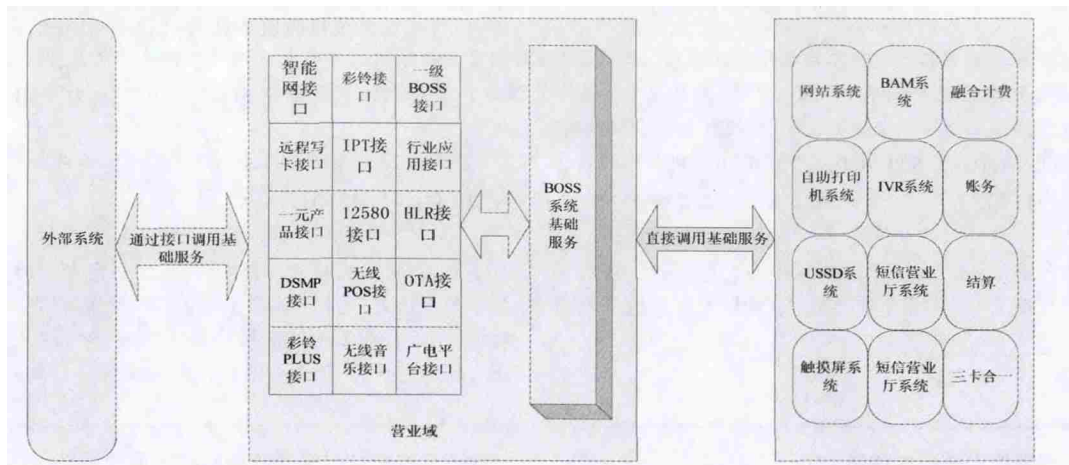


图1 业务支撑系统与外部接口图示

2 企业级应用集成平台架构组成

为了统一管理外部平台与业务支撑系统的对接服务,构建了应用集成平台。为业务支撑系统提供统一的标准化通道与外部系统进行交互,实现在各个应用系统与业务支撑系统间桥梁作用,实现跨系统业务交易处理。

(1)协议种类繁多,报文种类也非常多,基本一个接口一个报文规范。系统缺乏统一接口平台架构和接口规范,各个接口各自开发,接口不易复用,系统扩展性差。

(2)接口应用比较多,对应用安全性能考虑少,缺乏集中、分类化的管理,系统维护难度大。

(3)基础服务直接给外围系统,外围系统压力会直接传递给核心系统,导致系统运行不稳定。

应用集成平台由通讯总线和适配器构成。通讯总线是传输控制层,负责根据路由信息在功能请求者和功能提供者直接转发信息;协议适配器是应用接口层,负责接口标准化。具体结构如图2所示。

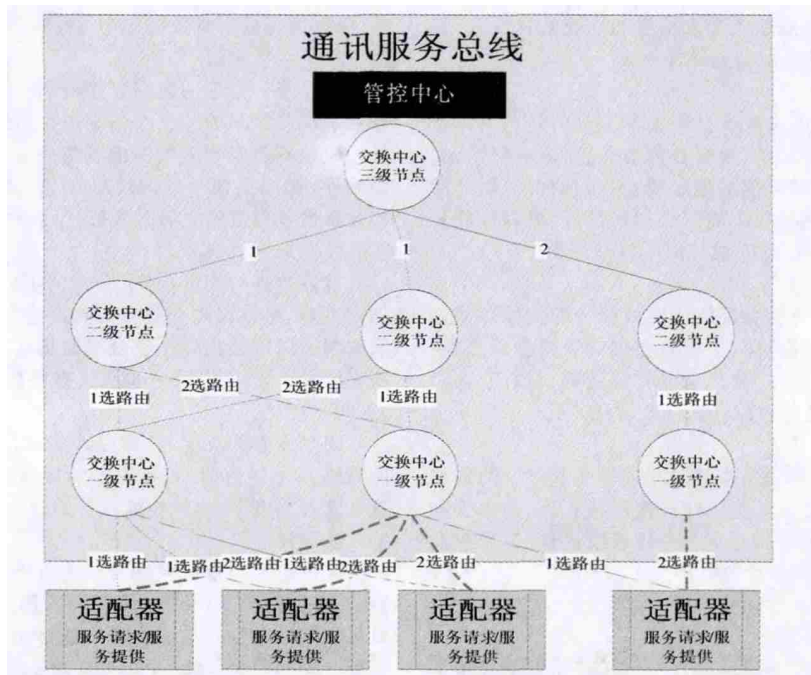


图2 应用集成平台架构图

(1)通讯总线处于集成平台核心地位,负责管理各个适配器的接入,根据路由信息在功能请求者和功能提供者直接转发信息。通讯总线由管控中心、交换中心组成,数据交互格式为MML格式。

①管控中心仅有一个,管理整个系统配置信息、路由信息,管理所有节点的状态,以及网络连接情况。管控中心不参与生产

数据的处理,如果有异常,不影响整个系统的正常运行。

②交换中心分三级管理,负责把客户端适配器的服务请求转发给服务端适配器,并把结果进行反馈。一级交换中心负责连接适配器;二、三级交换中心仅仅根据目的路由地址进行消息转发。客户端适配器向一级交换中心发起服务请求,一级交换中心根据目的路由地址,通过二、三级交换中心将请求消息转发给服

务端适配器。

③通讯总线内部及通讯总线与适配器数据交互格式采用 MML 键值对方式。

(2)协议适配器用于实现协议标准化。存在多种协议适配器,用于完成外部协议与内部协议的转换,实现协议的标准化。

①按照协议种类分为 HTTP+XML 协议适配器、SOAP 协议适配器、TUXEDO 协议适配器、TCP 协议适配器、数据库适配器。

②按照功能分类,根据每种协议适配器与通讯总线关系,分为客户端适配器与服务端适配器。客户端适配器作为交易发起方;服务端适配器作为交易受理方。

③协议适配器主要功能是数据格式转换功能,把外部协议转换为内部系统能够识别的 MML 格式,把内部 MML 格式转换为外部系统能够识别的协议格式。

3 企业级应用集成平台在业务支撑系统中的应用

通过通讯总线、适配器进行组装,建立应用集成平台,业务支撑系统与外部系统统一通过应用集成平台对接。针对不同协议接入的业务平台,只需要配置相关的适配器进行对接,实现业务支撑系统与外部平台的一体化管理。如外部系统对接使用 SOAP 协议接入,在应用集成平台部署一个 SOAP 客户端适配器、一个 SOAP 服务端适配器、一个 Tuxedo 服务端适配器。SOAP 服务端适配器调用外部系统服务;SOAP 客户端适配器接收外部系统调用;Tuxedo 适配器调用内部服务。实现业务支撑系统与外部系统间业务交互。具体如图 3。

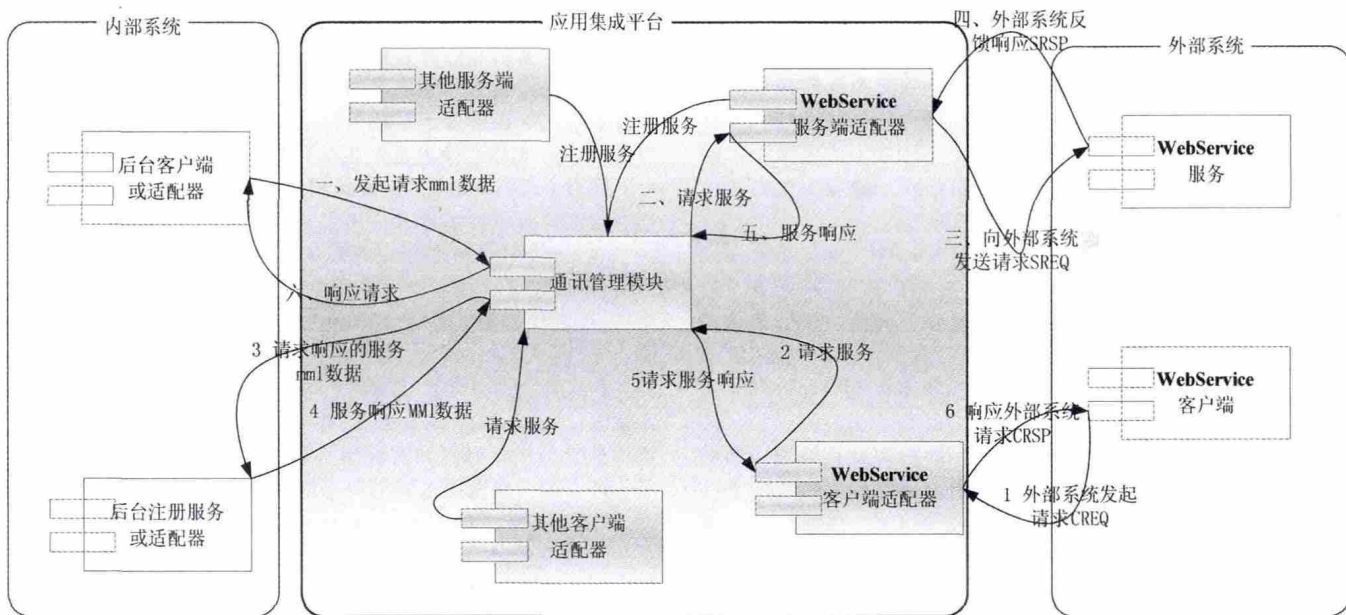


图 3 支撑系统通过应用集成平台与外部接口统一管理图示

4 企业级应用集成平台使用优势

在企业信息化管理快速发展过程中,系统专业分工趋势明显,系统功能与服务分散在各系统中进行管理。但是各系统间有时需要进行交互,实现服务及数据的共享。系统间服务集成成为企业信息化建设中必须面对的问题。企业级应用集成平台的建设就是满足企业信息化管理中系统间服务集成要求,并体现出如下优势。

(1)接口的统一标准化管理:应用集成平台统一对外部平台接入进行管理,满足外部应用系统与业务支撑系统间各种交易

3.1 实现业务支撑系统调用外部系统服务流程

(1)业务支撑系统客户端程序通过 API 向总线发送服务调用请求。

(2)通讯总线根据路由信息、把消息把服务请求信息转发给 SOAP 服务端适配器。

(3)服务端适配器把请求信息 MML 串转换为 SOAP 报文传给外部系统。

(4)外部系统接收服务请求,把服务处理结果反馈给服务端适配器。

(5)服务端适配器把 SOAP 报文转换为 MML 串并转发给通讯总线。

(6)通讯总线把处理结果 MML 串传给业务支撑系统客户端程序。

3.2 实现外部系统调用业务支撑系统服务流程

(1)外部系统向 SOAP 客户端适配器发起服务请求。

(2)客户端适配器把请求转换为 MML 串后传给通讯总线。

(3)通讯总线根据路由信息把消息传给服务端适配器,服务端适配器调用相关服务。

(4)服务端适配器把处理结果通过 MML 串格式发给通讯总线。

(5)通讯总线把处理结果给客户端适配器。

(6)客户端适配器把 MML 串转换为 SOAP 报文发给外部平台。

实时调度;针对不同类型协议提供不同的适配器,实现系统协议标准化管理。

(2)系统的安全稳定性:外部系统必须通过适配器安全验证,才能接入业务支撑系统;通过各级交换中心调度,实现服务的负载均衡,确保系统稳定;针对每类协议提供适配器,相同协议可以共用适配器,代码复用高。

(3)系统配置化、组件化:当有外部平台接入时,根据需要在通讯总线配置路由,把客户端适配器、服务端适配器发布在系统上并进行参数配置,通过组件的安装就可以实现系统的对接。