计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2019,28(2):87−93 [doi: 10.15888/j.cnki.csa.006764]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

双网隔离环境两级应用移动平台的设计与优化①

钮　卿

(神华国能集团有限公司, 北京 100033)

摘　要: 移动应用技术已逐步在电力行业推广应用. 近年, 某发电集团在双网隔离环境下按照移动门户模式建成了模块化的统一移动平台, 标准功能以集团总部应用为主, 部分通用功能基层单位也可以使用. 本文在此基础上, 基于 4G 和 Wi-Fi 无线网络、Hybrid 移动开发技术、Nginx 反向代理技术、SSL VPN、安全隔离网闸等, 设计了统一标准并能柔性适应各单位本地业务需求的支持两级应用的集团级移动平台, 实现了不同网络环境下的无缝切换, 为双网隔离环境下支持两级应用的集团级移动平台建设提供了参考.

关键词: 移动平台; 双网隔离; 两级应用; 移动门户; 反向代理; 无缝切换

引用格式: 钮卿.双网隔离环境两级应用移动平台的设计与优化.计算机系统应用,2019,28(2):87–93. http://www.c-s-a.org.cn/1003-3254/6764.html

Design and Optimization of Mobile Platform Supporting Two-Level Applications in Dual-Network Isolation Environment

NIU Qing

(Shenhua Guoneng Energy Group Corporation Limited, Beijing 100033, China)

Abstract: Mobile application technology has been gradually applied in the electric power industry. In recent years, a power generation group built a modular unified mobile platform in accordance with the mobile portal model in dual-network isolation environment. The standard functions are mainly used by the group headquarters, and some general functions can also be used by subcompanies. On this basis, this study, based on 4G and Wi-Fi wireless network, hybrid mobile development technology, Nginx reverse proxy technology, SSL VPN, gap and so on, designs a group level mobile platform with unified standard which can support two-level applications and can be flexiblely adapted to the local business needs of each subcompany. Seamless handover is implemented. It provides a reference for the construction of a group level mobile platform which supporting two-level applications in dual-network isolation environment.

Key words: mobile platform; network isolation; two-level application; mobile portal; reverse proxy; seamless handover

随着 4G 和无线网络的普及, 移动应用技术得到了长足发展和广泛应用, 智能移动终端也日趋普及, 互联网与实体经济融合不断加深, 各行各业的办公模式也在发生深刻的变化[1–4]. 双网隔离环境下的传统发电企业管理信息系统由于受限于办公地点和信息内网, 只能通过内网办公电脑进行访问, 这使得员工一旦出差或离开工位就无法方便地处理日常工作. 通过建设移动应用系统, 使公司员工可以通过移动终端随时随地开展业务, 可以有效提高企业日常事务和生产运营管理的方便性及工作效率[5–7].

近年, 某发电集团在双网隔离环境下建成了模块化的统一移动平台, 标准功能以集团总部应用为主, 部分通用功能基层单位也可以使用. 随着基层单位本地个性化业务需求的不断涌现, 部分单位可将本地应用模块发布至集团公司移动平台, 但是存在以下问题: 由于系统没有专门针对两级应用进行优化, 因此无法较

① 收稿时间: 2018-08-06; 修改时间: 2018-09-05; 采用时间: 2018-09-11; csa 在线出版时间: 2019-01-28

完整地支持两级应用, 影响系统使用体验, 增加新模块建设难度和系统运维难度.

为充分发挥基层单位积极性, 有必要建立统一标准并能够柔性适应各单位本地业务需求的集团级移动平台. 目前相关研究报道尚少, 本文针对以上问题, 基于 4G 和 Wi-Fi 无线网络、Hybrid 移动开发技术、Nginx 反向代理技术、SSL VPN、安全隔离网闸等相关技术的应用, 对移动平台整体架构的完善、身份认证、接口服务和网络环境无缝切换等方面关键机制的设计与优化进行了探讨.

1 移动平台架构设计与优化

1.1 技术路线

为支持两级应用, 按照移动门户模式建设移动平台, 主要包括以下几个主要部分: 移动应用 (Application, APP)、移动代理服务平台 (Mobile Agent Server, MAS)、企业移动管理平台 (Enterprise Mobile Management, EMM).

与传统的移动应用部署方式相比, 移动门户可以为用户提供统一的企业移动应用安全入口. 移动门户内部采用模块化的业务应用管理模式, 所有业务功能作为移动门户的子模块, 根据权限和用户需求下载使用, 避免安装多个移动应用. 对于双网隔离下两级应用的移动平台, 移动门户模式更能够提高用户体验, 降低维护难度.

同时, 移动门户将技术类需求和业务类需求的实现分离, 有利于移动应用建设管理. 移动应用的整体框架和通用功能在建设移动门户时统一设计, 并向各业务模块提供通用的技术类服务. 新开发业务应用模块时只需要将重心放在业务功能的实现上.

1.1.1 移动门户 APP

移动应用采用 Hybrid 模式构建, 能够较大程度兼容不同品牌移动终端设备和操作系统, 开发人员不需要精通多种移动操作系统的复杂开发技术, 遇到无法统一的技术差异时也只需分别开发不同平台的插件作为补充, 从而使得主要精力专注于功能和业务实现. 通过 Hybrid 模式构建企业移动门户, 已经成为企业移动信息化的一种主流选择[3,4]. Hybrid 开发模型如图 1 所示.

Hybrid 开发模型综合了 Web App 和 Native App 两种移动开发模式的优点, 使用 HTML5 技术构建用户界面, 并具有访问设备的原生功能.

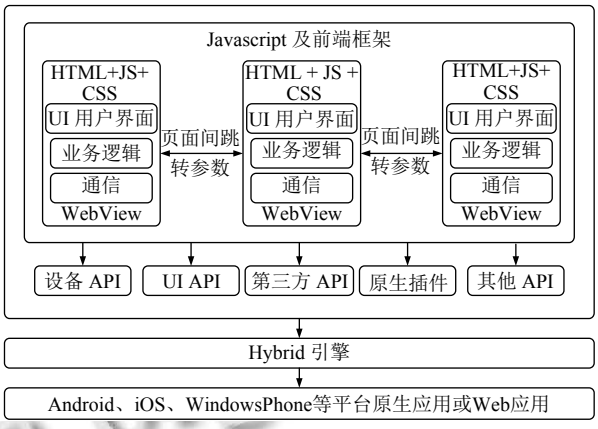

图 1 Hybrid App 开发模型示意图

本文使用成熟的 Hybrid 移动应用开发和打包引擎, 开发时前端以 Html5+javascript 为主, 基本实现一次开发, 多平台版本 APP 打包.

采用 VPN (Virtual Private Network, 虚拟专用网络) 和 SDK (Software Development Kit, 软件开发工具包) 提供的接口方式, 在开发过程中实现 VPN 客户端与移动门户 APP 的一体化集成, 为移动门户 APP 提供专属的 SSL(Security Socket Layer, 安全套接层) VPN 通道[5].

1.1.2 移动代理服务平台 (MAS)

采用 Node.js 技术构建移动代理服务平台, 为移动端使用企业内部应用系统、数据库等资源提供包含数据处理逻辑的代理接口, 优化任务并行处理, 避免阻塞操作, 同时可以使得 MAS 接口的开发语言与移动应用前端保持一致, 降低系统建设与维护难度[3,4].

对于新开发系统, 要求在建设时预留移动化业务接口. 对于现有业务系统, 为了在尽可能不修改系统的情况下实现移动化, 在对接时一般采用 Web 适配技术.

移动平台与业务应用系统集成关系如图 2 所示. App 调用 MAS 接口时, 后者会相应调用业务应用系统的业务接口, MAS 将返回的数据解析后, 交由移动门户 App 进行展现.

1.1.3 企业移动管理平台 (EMM)

使用支持集团级应用的成熟企业移动管理平台, 为企业提供对用户、设备、应用的准入与综合管理服务, 并在此基础上实现企业应用商店、移动接入控制、移动运行监控等关键功能. 移动管理平台应具备二次开发、集成业务管理后台、扩展服务的能力, 保障移动管理体系的完善和全面.

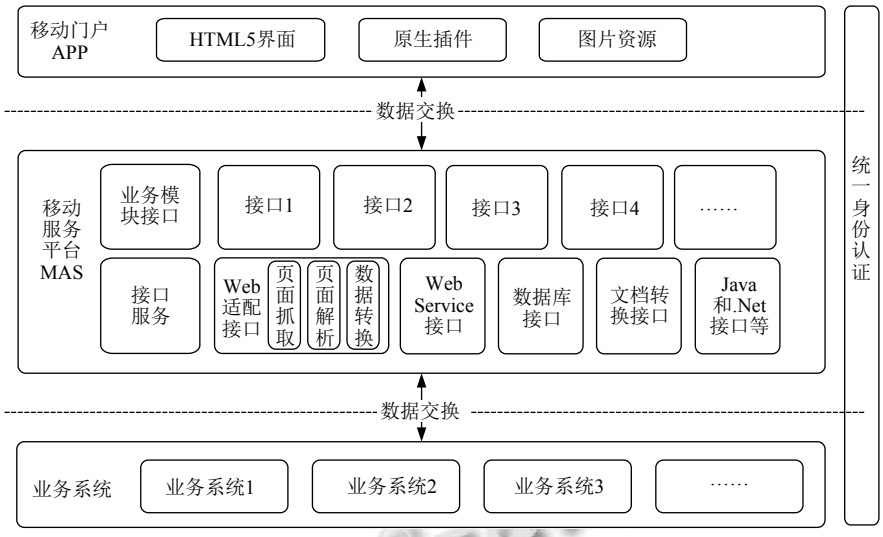

图 2 系统集成示意图

为支持两级应用, 应支持建立多级组织机构、多级管理权限、用户多组织机构授权. 集团公司管理员可以管理集团总部及各单位的用户、设备与应用模块, 基层单位管理员可以管理本单位的用户、设备与应用模块.

1.2 系统物理架构的升级

系统主要由 MAS 服务器、EMM 服务器、文档转换服务器、反向代理服务器、安全隔离网闸、SSL VPN、移动终端等关键节点组成[5–17], 网络接入方式主要包括移动网络接入和 Wi-Fi 接入, 如图 3.

在集团侧, MAS 服务器部署在集团内网核心业务区, 对内与集团业务服务器对接, 对外与移动终端、EMM 服务器对接; EMM 服务器部署在集团外网 DMZ 区, 对内与 MAS 服务器对接, 对外与移动终端对接. 通过 DMZ 区的反向代理服务器发布对外服务.

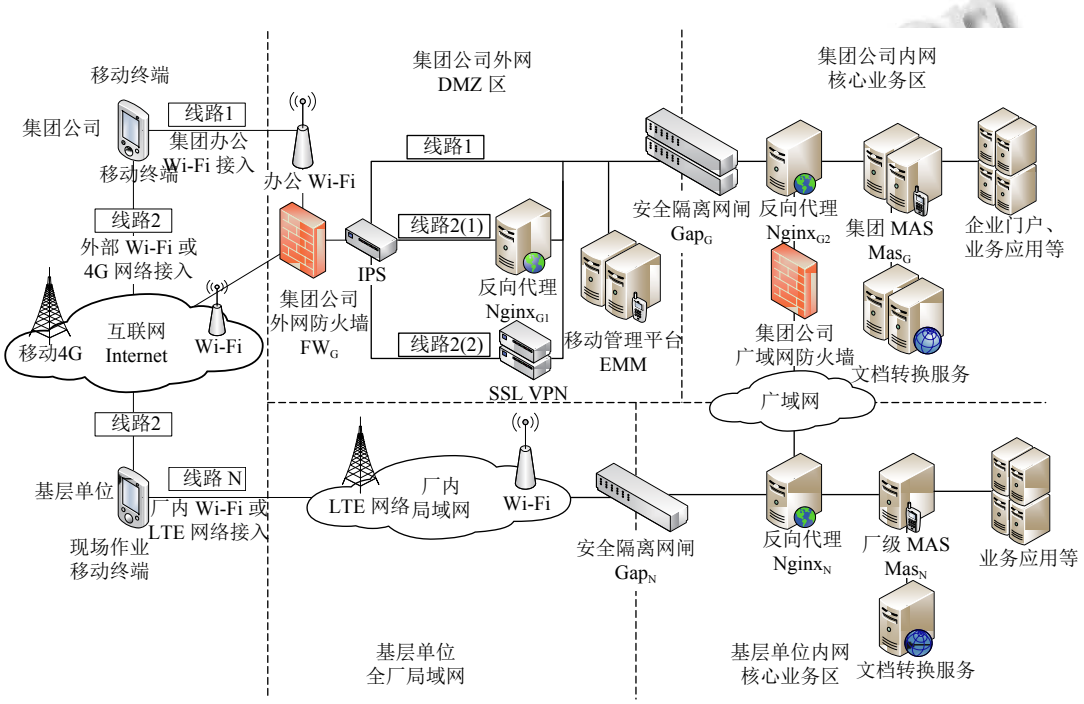

图 3 网络架构示意图

为解决基层单位无法在本地使用的问题, 各基层单位通过厂内局域网为移动平台提供新的接入通道. 在双网隔离环境下, 应部署安全隔离网闸和厂级 MAS 服务器. MAS 服务器部署在内网核心业务区, 对内与本地业务服务器对接, 对外与移动终端对接. 在集团和基层单位, 通过对安全隔离网闸、SSL VPN 等进行设置, 确保只能访问到内网的反向代理服务器.

网络线路升级后, 共有 2+*N* 条入口线路:

集团线路 1: 移动终端通过集团办公 Wi-Fi 接入, 可直接访问集团和各单位的 MAS 服务在集团侧反向代理服务器映射到安全隔离网闸 DMZ 区的地址.

集团线路 2: 移动终端通过移动网络或其他 Wi-Fi 的互联网接入集团侧.

(1) EMM 服务器均通过反向代理服务器代理.

(2) 接入 VPN 后, 访问集团和各单位 MAS 的反向代理服务器映射到安全隔离网闸 DMZ 区的地址.

各基层单位线路 *N*: 移动终端通过厂内 LTE 或 Wi-Fi 接入, 可直接访问集团和各单位 MAS 的反向代理服务器映射到安全隔离网闸厂内局域网侧的地址.

1.3 系统应用架构

系统应用架构包括提供基础服务的通用功能模块和业务功能模块[5–10], 如图 4.

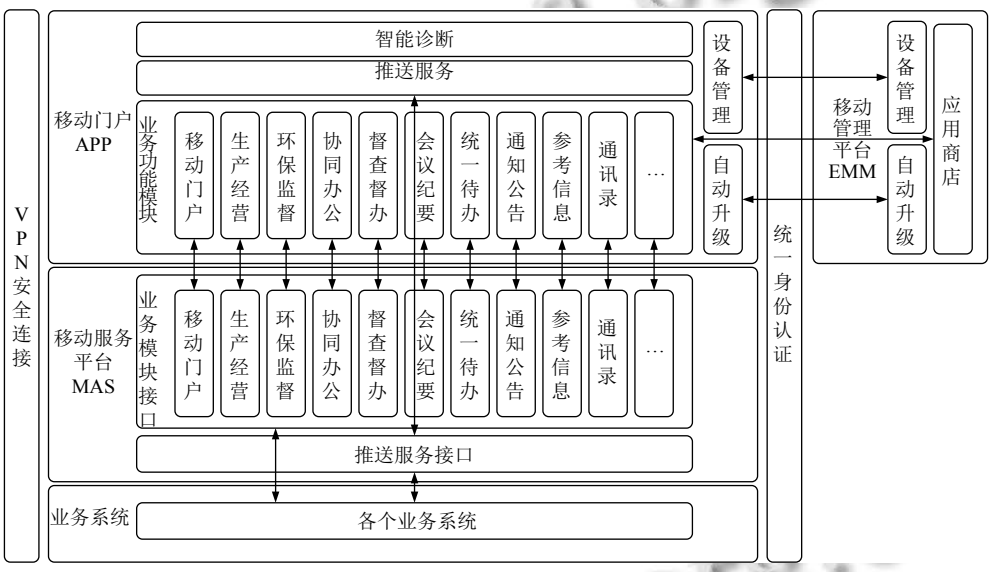

图 4 应用架构示意图

基础功能模块包括: 移动门户、VPN 连接、身份认证、智能诊断、推送服务、应用商店等.

业务功能模块包括: 集团统一建设模块例如生产经营、环保监督、协同办公、统一待办、通知公告、生产管理、通讯录等. 基层单位包括例如移动点巡检、到岗到位、生产监控信息等.

1.4 系统安全架构

系统安全架构应从网络、应用、数据、终端等多方面进行设计, 形成完整的安全防护体系[11–16].

(1) 网络安全: 通过 SSL VPN 建立安全网络接入通道, 采用 WPA2-PSK(AES) 加密算法管理设备接入办公 Wi-Fi, 并做设备准入控制. 通过安全隔离网闸、VPN 等设置最小访问范围.

(2) 应用安全: 通过反向代理设置最小服务访问范围. 采用多重身份认证机制, 设置设备白名单并进行绑定. 采用应用级 SSL 加密. 密码设置防穷举攻击机制. 采用系统用户停用机制. 可根据需要将用户锁定. 对用户操作进行详细的记录.

(3) 数据安全: 按照最小缓存策略设计, 内部文件以加密图片形式传输并自动清理缓存. 用户名、密码均加密存储. 应用传输时数据使用高强度算法加密.

(4) 终端安全: 移动终端设置例如开机密码、锁定屏幕等机制, 防止手机终端被盗用带来的隐患. 安装安全防护软件, 减少病毒威胁, 阻止越权访问, 并实现重要数据的远程擦除功能.

2 移动平台两级应用优化研讨

为了满足对基层单位个性化业务的完整支持, 既

统一标准又能够柔性适应各单位本地业务需求, 保证广域网中断的情况下还能够部分使用业务, 移动平台升级为多网络入口, 也相应增加了技术复杂性. 为实现不同网络环境下的无缝切换, 移动平台的两级应用按照以下原则进行优化:

(1) 用户无论属于集团总部还是基层单位, 都可以使用具有权限的业务功能.

(2) 移动端无论处于集团总部、基层单位还是其他网络位置, 都能够以最佳方式正确访问具有权限的业务功能.

(3) 自动判断当前网络环境, 采用适用的方式保证系统的持续访问.

本文从身份认证、接口服务、网络环境无缝切换等方面对两级应用优化进行讨论.

2.1 身份认证的优化

身份认证主要包括以下两类: 集团公司业务和部分基层业务接入的集团的统一身份认证, 其他基层单位业务采用的本地认证. 按照以上原则, 身份认证需要做以下优化:

(1) 初始化身份认证: 在首次使用移动门户 APP 时, 应通过集团入口进行认证. 建立 VPN 通道后, 使用集团统一身份认证帐号进行认证, 由集团 MAS 提供身份认证接口. 如果认证成功, 则在 EMM 中将此移动设备加入白名单, 并绑定身份, 以后启动移动门户 APP 时只需定期更新集团统一身份认证信息, 但不需要频繁输入. 移动端相应增加保护密码, 例如文本密码、手势密码或指纹密码等.

(2) 日常身份认证: 无论用户的网络状态如何, 客户端都会在后台向集团 MAS 接口发起统一身份认证. 如果通过认证, 则可使用全部集成到集团的业务模块. 对于基层单位本地在线业务模块, 则另行通过本地 MAS 进行身份认证. 对于需要离线使用的模块, 在该模块每次认证成功后, 允许免登录使用, 待下次联网使用时, 再次进行身份认证, 通过认证后同步业务数据. 如移动门户 APP 启动时由于网络原因未完成某类型的身份认证, 则对应的模块不可用, 当网络状态发生改变时, 移动门户 APP 会再次发起身份认证, 通过认证后自动点亮相关模块.

2.2 接口服务的优化

为实现不同网络环境下移动接口服务的最大可用性, 方便使用和维护, 按照以下思路优化部署移动接口服务:

(1) 分别通过各单位 MAS 服务处理本单位侧业务, 即: 集团 MAS 为接入集团统一身份认证的所有系统提供业务处理接口; 基层单位 MAS 为其他本地业务系统提供业务处理接口. 这样, 若发生例如广域网中断的情况, 基层单位用户可以通过本地线路使用本地业务功能, 通过集团线路 2 使用已接入集团的业务功能.

(2) 每个网络线路上内网的反向代理服务器均发布集团和基层单位 MAS 的服务, 即: 集团反向侧代理服务器将集团 MAS 和各基层单位 MAS 的业务接口全部进行代理, 各单位反向代理服务器将集团 MAS 和本单位 MAS 的业务接口进行代理. 这样, 只要基层用户的移动终端能够接入本单位线路或集团线路中的任何一条, 都可以使用该用户具有权限的全部业务功能.

反向代理技术是由代理服务器作为应用服务的前置机, 接收用户的访问请求并转发到相应的应用服务器, 再将应用服务器的响应结果返回给用户, 反向代理过程对于用户是无感知的. 相比较于其他常用的反向代理服务软件, Nginx 是一款轻量级的产品, 其内存占用少, 业务扩展性强, 并发能力强, 具有很高的可靠性和稳定性, 可支持企业移动平台所使用的 HTTP 和 HTTPS 协议, 适用于企业级中小型应用, 在同类型的反向代理服务软件中表现较好[17].

本文中集团侧将 Nginx 反向代理服务器分别部署在 DMZ 区 ($Nginx_{G1}$)、内网区 ($Nginx_{G2}$). 每个基层单位在本单位内网区部署一台 Nginx 反向代理服务器 (用 $Nginx_N$ 代表). 通过配置 MAS 服务代理, 并提供统一的域名 $HOST_{mas}$, 无论用户处于集团网络还是厂级网络, 都可根据移动端不同的业务请求转发至不同的 MAS 服务端, 便于系统开发和维护.

2.2.1 集团接口服务的代理

集团接口服务的代理如图 5 所示.

(1) 集团 MAS 服务器 Mas_G 内网地址为 IP_{mG}, 对外提供业务接口、推送消息接口、管理后台三项服务.

(2) 集团反向代理 $Nginx_{G2}$ 地址为 IP_{nG2}, 在 $Nginx_{G2}$ 上配置 Mas_G 的代理访问至 IP_{mG}. 对 MAS 管理后台 URL 进行过滤, 只对外提供业务接口、推送消息接口两项服务.

(3) 厂级反向代理 $Nginx_N$ 地址为 IP_{nN}, 在 $Nginx_N$ 上配置 $Nginx_{G2}$ 的代理访问至 IP_{nG2}, 将集团业务接口发布至 $Nginx_N$.

(4) 安全隔离网闸 Gap_G 的 DMZ 端地址为 IP_{gG}, 在 Gap_G 上配置将内网 $Nginx_{G2}$ 地址映射为 DMZ 端地

址 IP_{gG} 和端口 $PORT_{mas}$, 将 MAS 提供的对外服务发布至外网 DMZ 区.

(5) 在外网 DMZ 区域名服务器和 VPN 移动应用环境配置中, 将域名 $HOST_{mas}$ 指向 Gap_G 的 DMZ 端地址 IP_{gG}. 确保通过办公 Wi-Fi 或 VPN 接入的终端使用统一的域名访问 MAS 服务.

(6) 反向代理 $Nginx_{G1}$ 地址 IP_{nG1}, 在 $Nginx_{G1}$ 上配置 MAS 代理访问至 IP_{gG}, 代理推送接口.

(7) 将互联网域名 $HOST_{app}$ 指向外网防火墙 FW_G 的互联网地址 IP_{fG}, 在 FW_G 中配置将 $Nginx_{G1}$ 绑定域名 $HOST_{app}$.

(8) 配置 $Nginx_{G1}$, 对 MAS 业务接口 URL 进行过滤, 只允许通过域名 $HOST_{app}$ 访问 MAS 服务接口, 只对外推送消息接口一项服务.

(9) EMM 的配置同理, 将自动升级、设备管理接口发布至互联网.

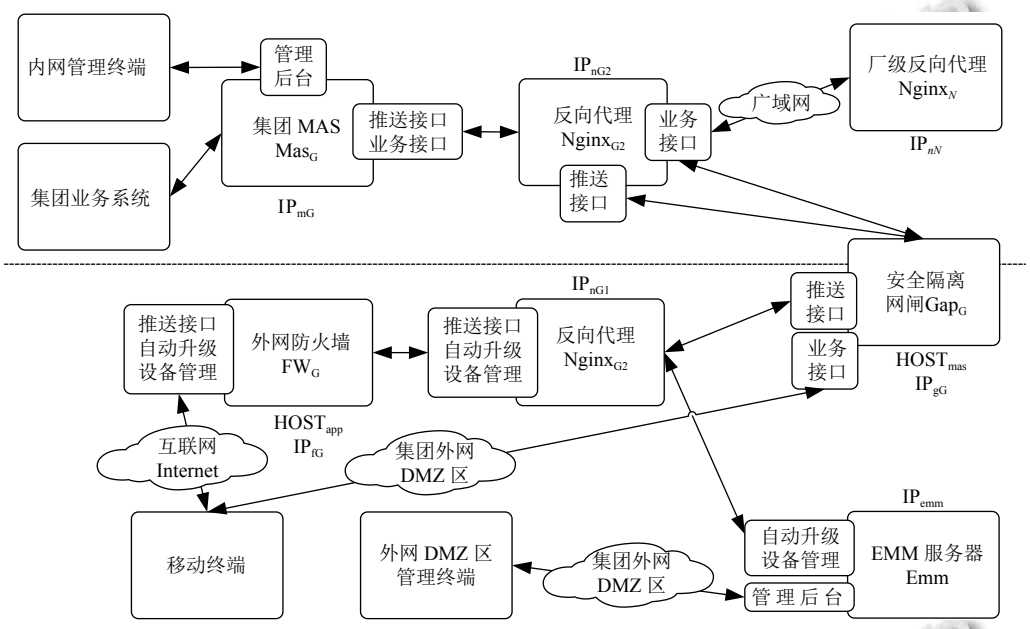

图 5 集团接口服务代理示意图

2.2.2 厂级接口服务的代理

厂级接口服务的代理如图 6 所示.

(1) 厂级 MAS 服务器 Mas_N 内网地址为 IP_{mN}, 对外提供业务接口、管理后台两项服务.

(2) 厂级反向代理 $Nginx_N$ 地址为 IP_{nN}. 在 $Nginx_N$ 上配置 Mas_N 的代理访问至 IP_{mN}, 代理厂级业务接口.

(3) 在 $Nginx_{G2}$ 上配置 $Nginx_N$ 的代理访问至 IP_{nN}, 代理来自于 $Nginx_N$ 的厂级业务接口. 对于多家基层单位, 以此方法分别配置厂级业务接口的代理.

(4) 厂级安全隔离网闸 Gap_N 的 DMZ 端地址为 IP_{gN}, 在 Gap_N 上配置将内网 $Nginx_N$ 地址映射为外部地址 IP_{gN} 和端口 $PORT_{mas}$. 将 MAS 服务 DMZ 区域名 $HOST_{mas}$ 指向 Gap_N 的 DMZ 端地址 IP_{gN}.

2.3 网络环境无缝切换的优化

用户无论处于移动网络、外部 Wi-Fi 还是办公 Wi-Fi, 在改变所处网络环境后, 系统都能够在新环境中自动连接, 实现用户基本无感知的无缝切换.

(1) 配置办公 Wi-Fi 列表: 在 EMM 服务上维护各单位适用的办公 Wi-Fi 列表. 移动门户 APP 完成用户绑定后, 根据用户所在单位下载相应的办公 Wi-Fi 列表, 每次接入 EMM 服务认证时, 检测是否有新版本的办公 Wi-Fi 列表, 如有则进行更新, 确保办公 Wi-Fi 列表处于最新状态.

(2) 网络状态切换时的处理策略: 当移动端接入网络状态切换后, 若未处于办公 Wi-Fi 下, 则自动尝试通过互联网 (集团线路 1) 建立至集团 VPN 的安全通道; 若处于办公 Wi-Fi 列表所包含名称的网络中, 则访问域名为 $HOST_{mas}$ 的服务端, 判断是否为办公 Wi-Fi. 若能够访问域名为 $HOST_{mas}$ 的服务端, 则处于办公 Wi-Fi, 可正常开展业务; 若不能访问, 则在下次网络状态切换之前, 都认为移动端处于非办公 Wi-Fi 下, 标记该

状态并自动尝试通过互联网建立集团 VPN 安全通道. 此时, 只要移动端能够访问互联网, 或处于企业内部办公 Wi-Fi 网络中, 都能够访问域名为 $HOST_{mas}$ 的服务端, 并通过当前线路的代理服务与 MAS 对接; 由于不同的 MAS 服务各司其职, 反向代理服务只是转发数据, 不另外生成会话, 所以网络切换后, 即使切换了代理服务也不会影响 MAS 的会话状态, 从而实现业务的无缝切换.

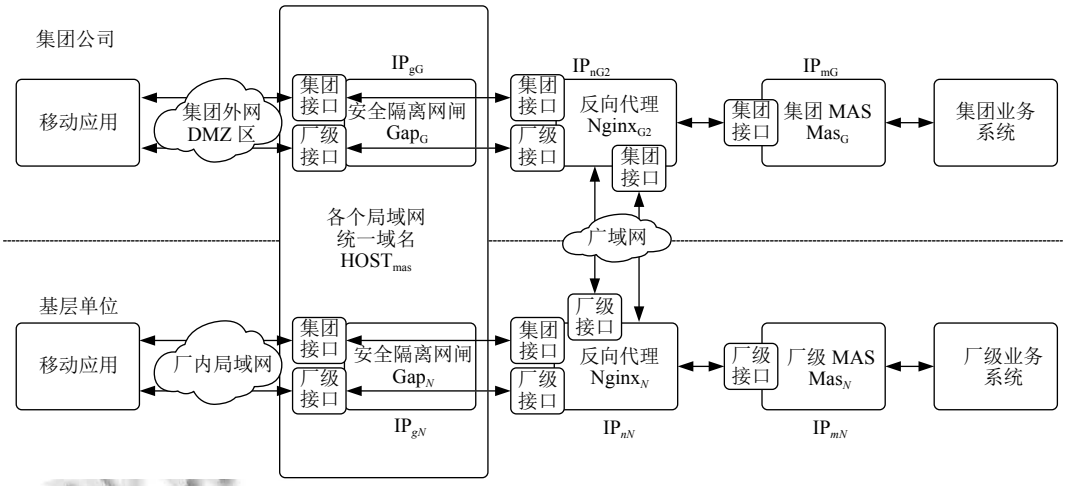

图 6 两级接口服务代理示意图

3 结语

本文在某发电集团企业的移动平台现状基础上进一步研究, 设计了双网隔离环境下支持两级应用的集团级移动平台, 通过网络架构升级, 以及对身份认证、接口服务和网络环境无缝切换的优化, 解决了系统两级应用的问题, 并进行了部分应用实践, 方案具有可行性, 为双网隔离环境的集团企业建设移动平台提供了一定的参考.

参考文献

1 王鑫. 移动应用 App 的发展研究. 内蒙古财经大学学报, 2017, 15(1): 114–117. [doi: 10.3969/j.issn.2095-5871.2017.01.027]

2 王鑫. Native App 与 Web App 移动应用发展. 计算机系统应用, 2016, 25(9): 250–253.

3 杜帅, 鄂海红, 许可. 混合移动应用开发模式的新策略. 软件, 2015, 36(6): 12–17. [doi: 10.3969/j.issn.1003-6970.2015.06.003]

4 王荣海. 基于 Hybrid App 技术的企业移动应用系统构建研究. 软件工程, 2016, 19(7): 46–49. [doi: 10.3969/j.issn.1008-0775.2016.07.014]

5 钮卿. 手机移动办公系统在双网隔离环境下的设计与优化. 电力信息与通信技术, 2014, 12(7): 109–114.

6 张云翔. 电力企业基建移动应用平台研究与应用. 电力信息与通信技术, 2016, 14(9): 94–98.

7 周志烽, 何超林, 梁超, 等. 电网调度移动平台的构建与应用. 电力信息与通信技术, 2014, 12(12): 91–96.

8 张向阳, 朱建生, 刘承亮, 等. 铁路企业移动应用平台的研究与开发. 铁路计算机应用, 2017, 26(9): 15–19, 23. [doi: 10.3969/j.issn.1005-8451.2017.09.004]

9 高嘉泽, 高强, 吴国全, 等. 面向移动应用的后端服务平台. 计算机系统应用, 2014, 23(2): 22–27. [doi: 10.3969/j.issn.1003-3254.2014.02.004]

10 苏凯, 吴广财. 移动管理驾驶舱离线访问研究与实现. 电力信息与通信技术, 2014, 12(2): 80–85. [doi: 10.3969/j.issn.1672-4844.2014.02.017]

11 赵永国, 张诗军. 电力行业移动应用安全体系关键技术研究. 电力信息与通信技术, 2017, 15(3): 20–26.

12 刘强, 杨维永, 刘金锁. 电力移动信息化安全研究. 电力信息与通信技术, 2015, 13(8): 83–88.

13 薛文婷, 马良, 耿海洋. 电网企业移动终端的应用及安全分析. 电力信息与通信技术, 2017, 15(10): 132–136.

14 陈希, 刘颖卿, 叶蕴芳. 构筑移动应用安全评测体系. 电信工程技术与标准化, 2015, 28(12): 11–16. [doi: 10.3969/j.issn.1008-5599.2015.12.003]

15 邹煜. 企业级移动应用平台建设与安全保障体系探析. 网络空间安全, 2016, 7(6): 80–82. [doi: 10.3969/j.issn.1674-9456.2016.06.024]

16 何慧萍, 张华兵, 李永攀, 等. 移动统一接入平台安全体系研究与应用. 电力信息与通信技术, 2014, 12(6): 114–118.

17 邓庚盛, 付爱英, 熊永春. Nginx 反向代理技术在移动应用服务架构中的应用. 科技广场, 2017, (9): 83–87.