**中国银联与上海银行  
基于SDN的下一代金融云网络联合研究与应用实践  
从分层分区传统架构向云网架构转型**

中国银联 上海银行

祖立军等 马永祥等

（上海市科委项目资助（17YF1425800）: 金融行业云关键技术研究及应用）

1. 引言

中国银联与上海银行就金融云与SDN技术研究等达成合作，其中中国银联的电子商务与电子支付国家工程实验室与上海银行数据中心以下一代金融云数据中心为蓝图，组成联合研究团队开展基于SDN的下一代金融云网络架构技术研究。

**联合研究团队认为：云网络架构是机构开展金融云基础平台建设最为核心关键的因素**，其主要体现如下方面;

* **首先，双模IT中网络是唯一必须兼容两种IT模式的平滑互通的基础资源。**为兼顾新技术、新架构、新模式于既有的传统信息技术体系结合，双模IT将是金融机构IT发展的主要形态，处于两种IT模式下的金融应用无必须共享服务器和存储的要求，但必须在网络层面实现互联互通。
* **其次，金融合规性与安全性在IT基础设施中主要体现在数据中心网络。**金融机构多区域隔离、应用间的强访问控制以及外部防护攻击均主要基于网络规划与专用网络设备应用措施。
* **最后，以软件定义网络为代表的新技术应用是云平台发展的必然趋势。**基于云计算、大数据与区块链等新技术的金融创新应用产生了新的数据网络交换模型，对应用所部署的数据中心网络环境提出了新的技术要求，软件定义网络技术效果与之契合，有助于推动金融IT向高效服务化的转型，从而提升金融机构的创新能力。

然而，由于网络技术变革难度高与应用影响性广等因素，当前在全球范围内金融机构云网络架构落地实践整体上还处于初级阶段，无标准化统一的架构实践参考。为此**联合研究团队经过近两年多的努力，提出了在当前金融数据中心网络架构下，应用SDN的云网参考模型，并予以落地实践验证**，其中主要完成工作包括：

* **金融云数据中心需求梳理与新架构网络设计原则规划。**结合当前金融行业网络架构现状分析，梳理了未来金融数据中心网络高敏捷、高弹性、高可管理、高可用以及高性能的“五高”要求，归纳总结了未来金融数据中心网络架构“面向服务理念、管理统一编排、资源池标准化、成熟技术集成再造创新”的四大设计原则。
* **定义**基于SDN的下一代金融机构网络**的标准化参考架构。**联合研究团队提出了“多数据中心间虚拟专网互联，数据中心内核心交换总线互通，传统分区、云网分区并存”的云网络架构模型，模型给出了网络管理平面与数据平面的标准实现架构，服务能力涵盖二/三层网络连通性能力以及负载均衡/防火墙L4-L7服务能力。
* **验证标准化参考架构的核心关键技术。**研究团队已基于开源技术通过自主研发的区域互联（Region Interconnect）SDN控制器实现了对核心交换网络（国际首创）与各分区的SDN控制器的协调控制，从而实现数据中心内网络资源池化以及网络资源弹性调度服务。

上述云网架构模型的应用可实现新一代符合金融行业云要求的网络架构，其效果主要包括：

* **平滑兼容传统架构。**可有效支持双模IT，可在保持传统网络架构稳定运行的前提下，支持SDN等新技术的前瞻性应用。
* **兼容异构网络技术。**通过自主创新的区域互联（RI）SDN控制技术，实现对厂商设备异构解耦，屏蔽不同厂商在SDN技术实现中的技术差异性。
* **网络多租户能力扩展性强。**网络租户能力不局限于单一网络设备区域，可有效扩展至异构设备区域以及跨数据中心区域。
* **安全合规等级不降低。**新模型设计之初即基于现有网络安全与合规性的要求考虑，新技术的应用严格遵守现有金融规范。

在研究过程中，我们认识到金融云计算技术研究是技术集成创新与产业协同创新的复杂系统工程，金融云计算技术的自主可控需要良好的产业生态支持，因此也同步与国内外产业界保持密切沟通，探索相关技术在金融行业范围内以工作组的形式深化联合研究，在工作组内共享技术研究成果，共同以工作组的团体力量与国内外云计算组织展开合作，推动金融云技术的研究与进步，加速金融科技的变革，支撑金融服务的创新发展。

1. 金融行业网络架构现状

金融行业网络建设历程与金融行业近三十年信息化过程密不可分，目前为止已经历多个阶段发展。

现阶段金融行业网络整体多以“两地三中心”架构为主。利用DWDM及高带宽专线构建高速转发“核心骨干网”用于数据中心间互联，数据中心作为骨干网接入节点。在核心骨干网框架上扩展延伸出“三级网”架构用于各级分支机构的汇聚，数据中心至一级分支机构间构建一级网，一级分支至二级分支机构间构建二级网，二级至三级分支机构间构建三级网。示意图如下：

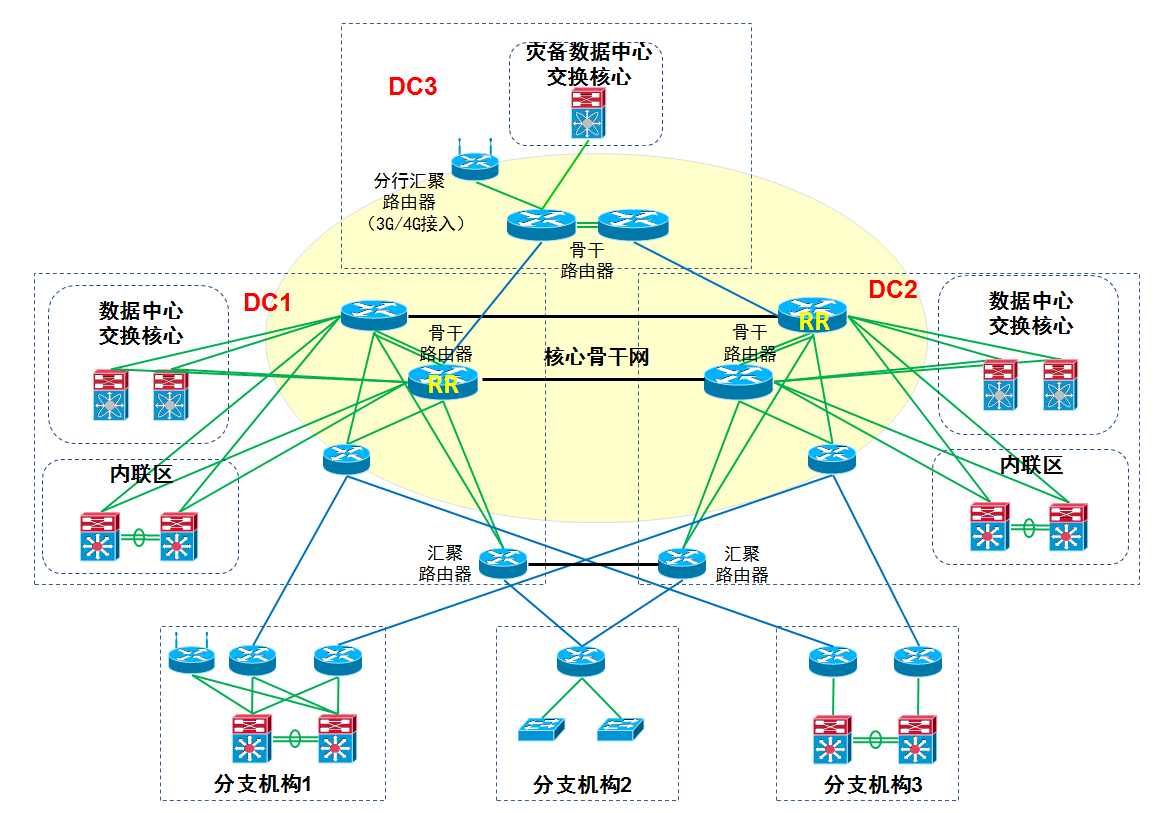


图1 阶段金融行业网络整体示意图

数据中心内部采用“总线型、模块化”架构，遵循“垂直分层、水平分区”的原则，根据应用系统种类不同、重要性区别、安全防护需求差异将网络划分为多个区域，通过高性能交换机构建交换总线，网络各分区通过总线进行互联互通，如下图：

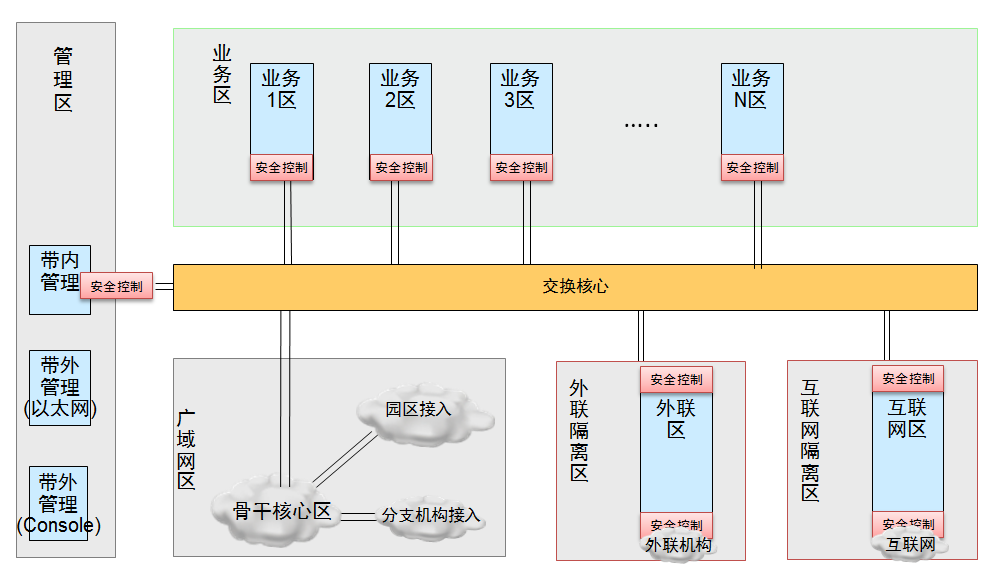


图2 数据中心内网络分区示意图

网络分区可划分为三大类：业务区、隔离区、特定功能区。

业务区：用于承载各类系统应用服务器及数据库服务器，应用系统根据特定原则划分至不同业务区。

隔离区：也称DMZ区，承载各类前置机，面向互联网或第三方机构提供服务。

特定功能区：如管理区承载监控系统、流程系统、操作终端等，用于数据中心维护；广域网区用户数据中心至骨干网的连通。

传统架构优点：安全、稳定、可靠、可扩展。

架构缺点：灵活性不足、竖井壁垒存在、自动化不高、建设成本高昂。

1. 金融数据中心网络面临的挑战

（一）面临的挑战

当前，“业务应用变革式创新发展”、“以云计算为代表的新技术应用”以及“金融IT成本与效率优化新要求”是金融数据中心网络发展面临的三大挑战。

首先业务应用发展对网络服务提出新的挑战，面向互联网方式的金融创新应用快速发展对网络服务提出更敏捷的服务要求，网络资源的开通与变更希望是从原本的周为单位提升到分钟级别，从而支撑应用快速投产。

其次，云计算等新技术在数据中心内越发应用广泛，其对网络连接也提出新的要求。为适应虚拟化技术，资源的漂移迁移能力，网络服务需要从物理机识别提升到虚拟主机识别，云的多租户特性要求在共享的物理网络设备下提供可独立解耦的网络地址路由空间，云弹性伸缩则要求网络有更高地弹性扩展能力，巨大的云平台规模，也要求云网络服务也必须具备足够的网络容量与健壮性。

再则，新常态下金融机构的运营压力要求IT架构可实现更高效与低成本，从纯商业“产品”解决方案向“自主”网络方案演进，金融数据中心网络技术应用更趋于开放，要求网络运维人员从单纯的人工维护解放出来，进入高效的自动化方式。

（二）未来金融数据中心网络应用需求

因此，结合上述发展的挑战与趋势，我们认为未来金融数据中心网络应用需求可总结为高敏捷、高弹性、高可管理、高可用以及高性能的“五高”要求：

高敏捷，实现业务快速上线，面对应用的变化达到资源的按需变更，通过新技术应用打破因重安全而舍效率的困局，在云计算新环境下安全与高效并重；

高弹性，一是内部弹性强化，打破竖井式架构中网络区域成为限制资源共享的壁垒，实现网络资源池整合与灵活共享与隔离，二是外部弹性兼容，支持新老架构并存，从而使原有网络可以平滑过渡到新架构；

高可管理，一是实现管理的体系的简化，支持多品牌的融合管理，二是实现管理自动化与智能化，使日常运维从大量人工维护的高工作量解放出来；

高可用，网络架构持续稳定影响金融数据中心全局服务能力，网络架构需要基于稳定可靠的技术构建，使网络服务具备7\*24小时业务连续性服务的能力；

高性能，面对秒杀等新业务场景等的极限服务能力，实现时延和带宽等关键指标的跨越式提升，同时注重资源的高效利用，用尽可能少的资源实现最大的性能服务。

1. 基于SDN的下一代金融机构网络设计与构想

（一）网络设计原则

SDN技术的应用对金融数据中心的架构是革命性的变化,因此下一代金融数据中心网络需进行针对性设计，我们总结未来金融数据中心网络需遵循以下四大设计原则：

面向服务理念，网络功能以服务、标准API接口的形式对外提供，网络系统内部以服务的形式进行自组织，从而提升对外服务能力，简化外部调用网络能力的复杂性；

管理统一编排，数据中心内网络二/三层连通、四/七层功能的管理界面统一视图，不同网络资源池的管理采用二级管理编排方式，即底层适配不同网络资源池管理操作、上层异构协调编排；

资源池标准化，打破传统网络竖井式架构，利用新一代的大二层技术构建资源池，在不扩大广播域、不增加二层环路风险的前提下提升计算、存储资源调动灵活性。

成熟技术集成再造创新，基于网络技术平滑兼容的要求，对基础可扩展网络技术与协议进行继承，组合现有技术进行集成创新，创新而不失稳定，保证网络架构的全局稳定。

（二）金融云网架构模型设计与构想

（1）管理控制平面模型

传统网络中各功能组件，如交换机、防火墙、负载均衡，通常采用不同的设备供应商解决方案，各产品管理接口存在差异（CLI、UI接口各不相同）、普遍不支持API接口。设备参数设置、配置调整大量依赖人工，且对于维护人员的专业技能要求较高。在此背景下，网络的服务化、自动化实现难度巨大，难以实现单一的工具或平台对全网设备进行统一管理和服务发布。

随着产业技术的发展，网络产品制造商也逐渐改变产品发展方向，由原先的封闭式设备向接口开放的方向发展。现阶段，业内越来越多的产品开始支持Restful API接口，管理模式不再局限于传统的CLI及UI接口。

数据中心新架构中，为了实现网络服务化、自动化、统一编排调度等目标，除了要求网络各组件支持API接口、可编程等功能特性外，我们认为在管理控制平面，还需对各品牌网络的API接口做进一步抽象，通过云网控制平台建立标准网络服务模型，并与各网络组件对接。一方面 ，实现网络服务接口的标准化，统一网络对外接口，屏蔽不同品牌设备接口的差异性，简化上层云管理平台的开发难度。另一方面，将复杂的网络参数隐藏，网络各组件的技术实现、参数设置仍由专业网络工程师完成，上层构建云管理平台专注于服务流程、业务编排、工作流调度、网络标准服务调用等。

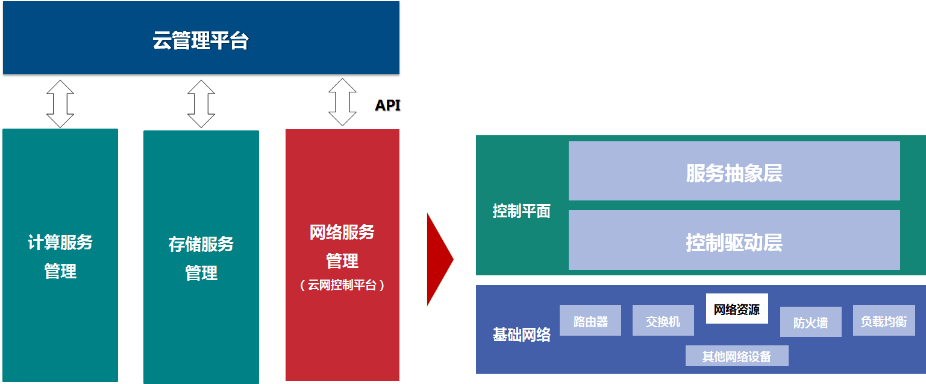


图3 云计算管理平台下的网络平台控制架构

云网控制平台又可分为两个层次，分别为服务抽象层和驱动控制层。

服务抽象层负责将网络资源抽象成标准的网络服务和模型，例如提供创建网络、创建路由器服务，同时对上层平台提供标准的网络服务API接口。

控制驱动层负责将标准的网络服务在具体的产品上实现，并将上层的API接口翻译成网络组件可识别的接口，实现对网络组件的参数调整。

（2）交换网模型

传统交换网络稳定有余但灵活、高效不足。各网络分区之间计算、存储、网络、机房物理环境等资源均为独享模式，不同分区之间计算宿主机无法共享资源，虚拟机不允许在不同分区宿主机间漂移，计算资源利用率下降。中小型金融机构交换网及各功能组件以普遍采用万兆级设备，设备性能强劲，但出于安全性、可靠性及合规性的考量，金融机构数据中心网络分区数量无法减少，在客户群规模、交易量不大的情况下，网络资源利用率普遍较低。在机房空间利用率上，各类设备的摆放需综合考虑布线、TOR交换机部署、电力、制冷等诸多因素，难以实现灵活部署。若采用传统技术，例如大二层，试图解决上述问题，又会造成广播域的放大、二层环路风险增加，对于后续运维造成巨大压力，得不偿失。

因此，我们认为新的交换网架构需在不增加运维风险的前提下提升计算、存储、机房空间资源的利用率。同时引入租户的概念，对一个交换网络进行隔离划分，对于单个金融机构可用于实现部分传统网络分区的合并部署，也可用于多金融租户的合并部署。

金融数据中心新交换网架构仍采用总线型架构，保留传统分区、传统应用接入，新增多个云网分区用于新应用上线或存量应用迁移。在风险可控的前提下，对部分功能相同的网络区域进行合并部署，例如多个业务区合并为一个云网分区，多个隔离区合并为另一个云网分区。

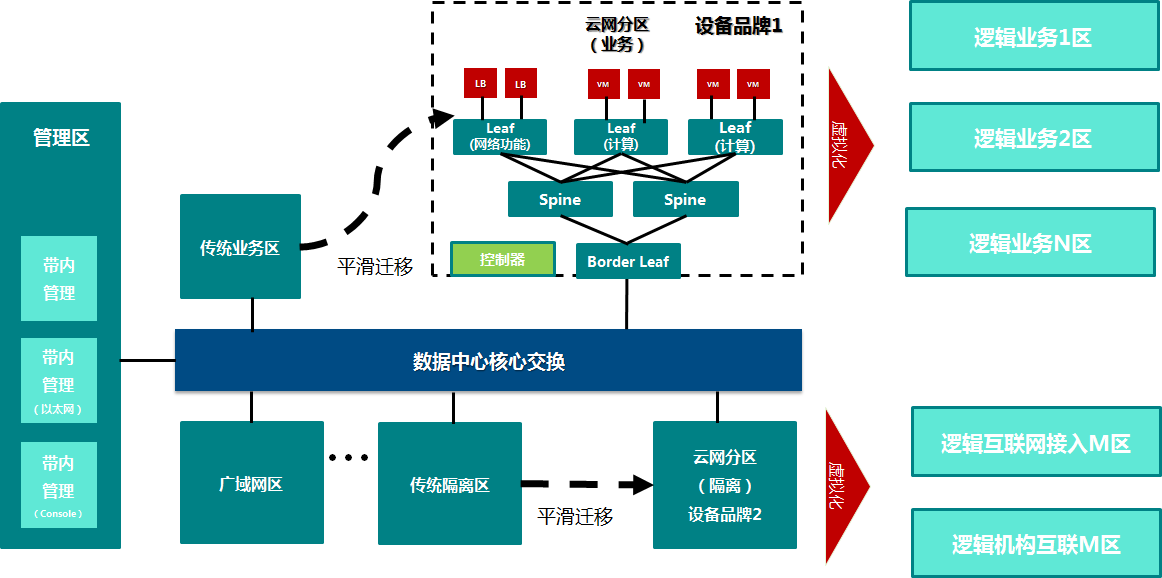


图4 云网模型架构

一个云网分区内由同一品牌的SDN设备组成，内部采用Vxlan分离Underlay、Overlay网络，实现网络物理架构与逻辑架构的解耦。采用Spine+Leaf的物理结构，其中计算Leaf接入提供虚拟机的计算服务器资源，网络功能Leaf接入负载均衡、防火墙等网元服务设备资源，Border Leaf负责与数据中心核心交换设备互联， 云网分区内由Spine设备负责各Leaf之间的流量互通，每个云网分区由其自有的控制器进行管理控制。

（3）分区之间互联模型

数据中心核心交换网络则是由独立交换设备组网，不同云网分区可能使用不同的SDN解决方案、协议与技术，云网分区内部的Vxlan标签在数据包出区域后被剥离，因此云网分区之间在Overlay层面无法实现互通。

上述数据中心内的组网模型与功能设计的挑战主要在于如何将存在于不同云网分区的租户流量进行识别，从而保证通过核心交换网络后，云网分区可以正确将IP地址重用的多租户流量转发至正确的租户资源。经过评估，我们认为传统技术中的VRF（虚拟路由转发表）或MPLS-VPN(基于多协议标签交换的虚拟网络)技术能很好的解决多个云网分区之间租户信息传递的问题，可将一个VRF或VPN网络抽象成一个区域互联路由器，用于连接同一租户不同逻辑区域。

同时，我们提出了一种区域互联SDN控制技术，实现对核心交换网络与各云网分区的SDN控制器的协调控制，实现多租户信息标识的传递的隧道能力。

图5介绍了在数据转发平面的设计思想，每个租户在出各自云网分区时，送入不同的虚拟路由表VRF（或VPN）进行转发，VRF是交换机内部隔离不同路由转发的虚拟化技术，实现了虚拟机的一虚多能力。



图5 RI数据平面转发设计图

在相应控制平面，我们设计了一个RI控制器实现对核心交换网络的自动化配置能力，其包括2大功能，一是根据租户变动情况动态创建配置VRF及其相关配置，二是实现在不同SDN 云网分区资源动态变化情况下，路由地址动态发布，以便保持动态变换的网络资源的连通性。

图6给出了RI控制器的架构设计，其通过netconf协议管理核心交换网络的设备，同时也通过适配不同SDN控制器的API接口定时或触发读取相应云网分区的动态资源信息。在跨异构SDN新租户创建过程中，则会自动根据前述数据转发平面的设计创建相应VRF通道，在有新网段资源创建时，触发RI控制器通过SDN控制API查询新增网段信息，并通过OSPF动态路由注入的方式更新核心交换网络中的VRF路由表信息，同时我们设计的RI控制器定时任务，定时查询SDN的网络资源信息，对比出已删除的网络资源信息，进行路由表清理工作。



图6 RI控制器控制平面设计图

在具体研发过程中，我们考虑到了核心网络设备支持的不同操作管理协议，以及未来不同合作伙伴今后提出新的隧道协议应用方式，因此在代码架构上我们支持了不同设备控制方式和隧道协议的扩展能力，以便未来完善优化。

（4）防火墙与负载均衡模型

防火墙及负载均衡用于提供四到七层网络服务，实现逻辑区域之间的安全隔离、服务器流量分摊。

金融云网架构模型中，可将防火墙及负载均衡等硬件资源进行池化部署，并按需进行调度。通过云控制平台实现防火墙、负载均衡资源池的统一管理。随着VNF技术的日益成熟，在未来，负载均衡和防火墙将作为VNF接入到不同业务逻辑区域当中，实现流量的合理编排和调度。

（三）两地三中心模型构想

在金融行业普遍采用“两地三中心”的高可用场景下，金融行业云平台的网络服务也必须支持跨数据中心的网络多租户能力。

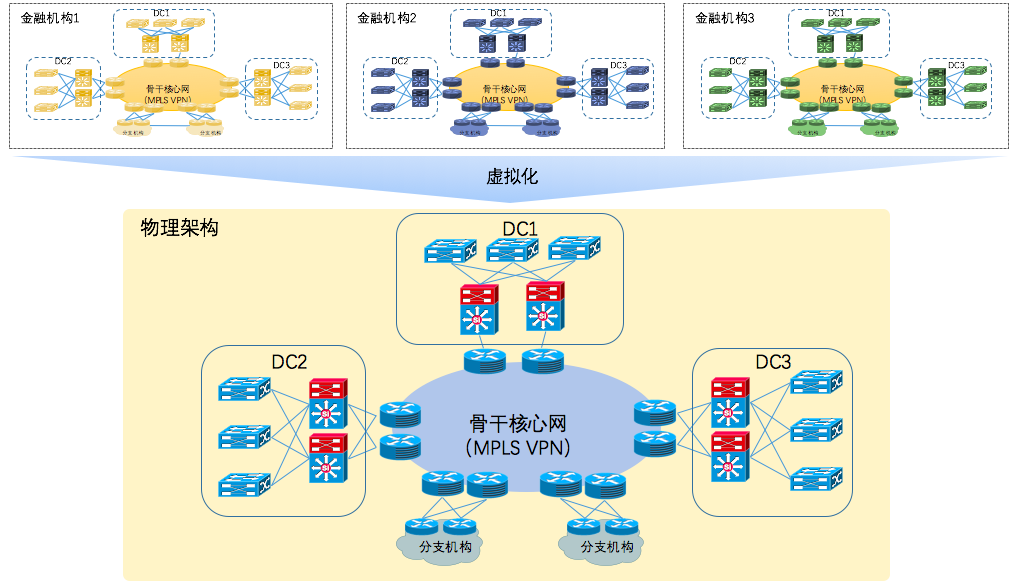


图7 两地三中心模型

在设计中可沿用现有骨干网的设计思路，并引入MPLS VPN技术，将同一租户的流量引入一个VPN网络中，实现单一租户可调用的资源范围覆盖所有数据中心，并支持分支机构的接入。同时利用MP-BGP丰富的选路能力以及QoS技术，实现租户信息跨数据中心传递，租户之间、应用流量之间相互隔离。

1. 原型实践情况

基于以上设计构想，研究小组就单中心模型进行原型验证，详细情况如下：

（一）物理架构概述

图8展示了的原型平台物理架构图，交换核心区域由华为三层交换机组成，下联2个不同品牌的云网分区，云网分区1为华为设备，云网分区2为思科ACI设备，根据不同云网分区IT服务商的合作沟通，负载均衡和防火墙的物理接入位置稍有不同，华为云网分区内负载均衡和防火墙接入网关组，思科云网分区内负载均衡和防火墙接入专用功能Leaf，但逻辑网络架构保持一致。

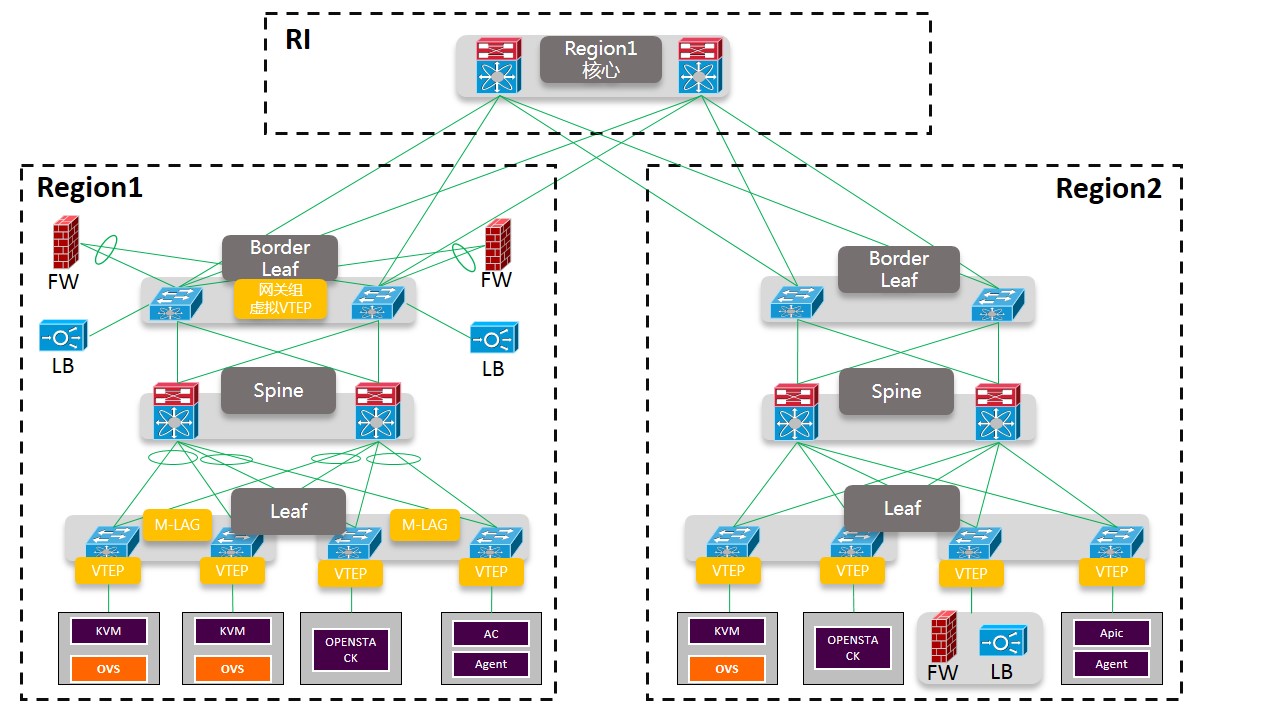


图8 原型平台物理架构图

我们在中国银联与上海银行联合研究的数据中心实验环境搭建了原型平台，平台由华为、思科两套异构SDN云网分区构成，同时也配备了相应的负载均衡和防火墙资源，平台设备列表如表1：

表1：原型平台设备列表

|  |  |  |  |
| --- | --- | --- | --- |
| **分类** | **厂商** | **设备类型** | **设备型号及版本** |
| SDN云网分区 | 思科ACI | 控制器 | APIC 2.1.3 |
| Spine | N9K-C9396PX |
| Leaf | N9K-C9336PQ |
| 华为AC | AC | AC 2.0 |
| Spine | CE6851-48F6Q |
| Leaf | CE6850-48P4Q |
| 核心路由设备 | 华为 | 三层交换机 | CE6850-48P4Q |
| 防火墙 | 思科 | ASA | ASA 5512 |
| 华为 | USG | USG6650 |
| 负载均衡 | F5 | BIG IP | BIG-LTM-1600 |

平台基于OpenStack、OVS、Centos等开源软件进行研发，相应软件版本情况如表2：

表2：软件版本情况表

|  |  |
| --- | --- |
| **软件** | **版本** |
| OpenStack | L 版本 |
| OVS | 2.4.3 |
| Centos | 7.0 |

（二）管理控制平台概述

使用OpenStack作为云控制平台，起到了承上启下的作用,向上暴露标准化的API给到多租户业务调度。另外一方面它通过底层SDN控制器、防火墙驱动、负载均衡驱动和RI模块，实现对下层物理网络资源的抽象、隔离和调度。

（三）云网分区和云控制平台集成

云网分区架构下，需要管理的四种资源：二层网络（思科APIC和华为AC）、三层网关、防火墙和负载均衡。云网分区和云管理平台集成的一般有以下两种模式：

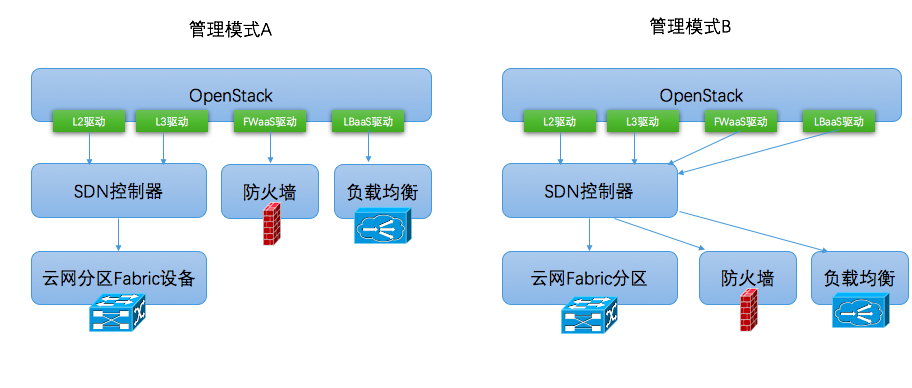


图9 OpenStack集成SDN云网分区技术模式

A模式通过SDN控制器驱动二层和三层，四层以上设备通过OpenStack Neutron直接管理，B模式通过SDN控制器驱动所有设备。我们现有的防火墙和负载均衡分别是思科的ASA防火墙、华为的USG防火墙以及F5负载均衡设备，下表是两种设备通过A模式和B模式下具备的驱动具备现状：

表3 设备和OpenStack集成驱动现状

|  |  |  |  |
| --- | --- | --- | --- |
|  | **A模式** | **B模式** | |
|  | OpenStack直接驱动 | 通过思科SDN控制器（APIC）进行管理 | 通过华为SDN控制器（AC）进行管理 |
| 思科ASA防火墙 | × | × | × |
| 华为USG防火墙 | × | × | √ |
| F5负载均衡 | √ | × | × |

我们选择了A模式和B模式混合的方式进行组网：

－ 思科ASA防火墙我们重新开发了OpenStack FWaaS驱动进行管理（A模式）

－ 华为USG防火墙通过华为SDN控制器进行管理（B模式）

－ F5负载均衡通过F5官方提供的OpenStack驱动进行管理（A模式）

在以上集成的基础上，我们开发实现了网间互联的RI模块，用来完成对核心交换机的策略下发，最终软件驱动的架构如下：

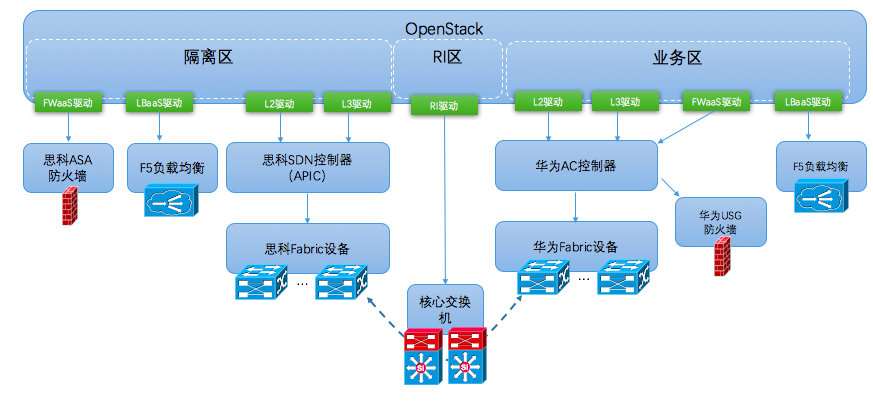


图10 原型集成驱动实现方式

下面我们将详细介绍每个模块的具体集成。

（1）思科APIC和华为AC的整合

OpenStack对接思科APIC和华为的AC SDN控制器，需要在原生OpenStack的基础上，在控制节点、网络节点和计算节点上做配置的变更。

表4思科APIC和华为AC的整合技术实现表

|  |  |  |
| --- | --- | --- |
|  | **思科ACI** | **华为AC** |
| OpenStack版本 | Liberty | |
| SDN控制器版本 | APIC2.0 | AC2.0 |
| 暴露给OpenStack的网络模式 | 只有一种选项：OpFlex模式 | 有三种选项：VLAN、VXLAN和GRE |
| 底层网络模式 | VLAN、VXLAN和GRE | VLAN、VXLAN和GRE |
| VLAN/VNI/Tunnel ID 分配方式 | 通过SDN控制器分配 | 通过OpenStack分配 |
| 控制节点配置 | －安装厂商APIC API并激活  －替换原生二层ML2驱动为厂商ML2驱动  －添加厂商L3驱动 | －安装厂商AC API并激活  －替换原生二层ML2驱动为厂商ML2驱动  －添加厂商L3驱动 |
| 网络节点配置 | －安装原生DHCP服务，但DHCP驱动替换成厂商的  －停止原生OVS代理，替换成厂商提供的OVS代理  －安装厂商提供Neutron OpFlex代理  －停止原生L3代理  －停止原生metadata代理 | －安装原生DHCP服务，不停止  －安装原生OVS代理，不停止  －无其他厂商定制代理需要安装  －停止原生L3代理  －原生metadata代理不停止 |
| 计算节点配置 | －安装厂商提供的OVS代理, 停止原生OVS代理  －安装厂商提供Neutron OpFlex代理 | －安装原生OVS代理  －无其他厂商定制代理需要安装 |
| DHCP驱动 | 厂商提供 | OpenStack原生驱动 |
| DHCP本地代理 | 实现 | 未实现 |
| Metadata本地代理 | 实现 | 未实现 |
| 分布式SNAT | 实现 | 未实现 |
| 分布式网关 | 实现 | 未实现 |
| 策略下发逻辑 | 计算节点和网络节点上的Neutron OpFlex代理会同步Neutron中的虚拟网络资源，生成Endpoint文件，通知agent-ovs读取，agent-ovs通过OpFlex协议到leaf节点上查询对应EPG的信息，然后通过OPENFLOW协议对OVS完成流表的下发。 | 复用OpenStack策略下发逻辑 |

（2）F5负载均衡集成

在OpenStack LbaaSv2模型中，负载均衡服务被抽象成loadbalancer，listener，pool，member，health monitor五种虚拟资源。一个loadbalancer下可以挂载多个listener，不同listener监听端口不同，一个listener下挂载一个pool，一个pool挂载members和health monitor。这些虚拟标准资源和F5资源的对应关系如下：

表5 F5负载均衡OpenStack资源映射表

|  |  |  |  |
| --- | --- | --- | --- |
| ＃ | **OpenStack抽象资源** | **F5对应资源** | **备注** |
| 1 | Loadbalancer | Partition  Router domain  Vlan  Snat pool  Selfip | Partition和router domain用来进行资源的隔离 |
| 2 | Listener | Virtual server  Profile |  |
| 3 | Pool | Pool | F5创建Pool时会更新virtual server的session-persistence,将pool挂载到virtual server上 |
| 4 | Member | Node | F5生成node时会更新pool中的member |
| 5 | Health monitor | Health monitor | F5中对应生成health monitor时会更新pool中的health monitor |

LbaaSv2 Driver将OpenStack中虚拟负载均衡资源通过RPC的方式发送给F5 agent，一个F5 agent可以管控一台F5设备、HA模式F5集群或者Cluster模式F5集群，同时F5 agent的分布式部署方式使得F5设备的横向扩展能力得到提升，通过LbaaSv2 Driver中的调度算法，将OpenStack中虚拟负载均衡资源合理的分配到不同的F5设备当中。

在和华为AC集成的时候，F5的管理通过 OpenStack进行调度，再通过AC中的L2BSR的方式接入到AC网络中。

在和思科ACI集成的时候，F5的管理通过 OpenStack进行调度，再将F5设备通过ACI中的Physical Domain方式接入到ACI中。由于ACI将虚拟网络类型变成了OpFlex类型，且该虚拟网络的VLAN（或者VNI）由APIC进行分配，这样导致OpenStack Lbaas在给F5下发配置时因为缺少VLAN或者VNI的信息而下发失败，需要通过修改F5的代码支持OpFlex类型来支持下发，或者启用F5提供的Global Route模式来解决。

（3）防火墙集成

和负载均衡一样，OpenStack为防火墙服务提供了V1.0和V2.0两种API模型， FWaaS 2.0在社区M版本中提出，现在仍在开发中，因此我们采用FWaaS 1.0 模型和防火墙设备进行集成。

同样的，防火墙服务被抽象成多种虚拟资源，分别是firewall，policy和rule。一个firewall可以关联应用到多个router，一个firewall使用一个policy，policy是rule的集合。和ASA防火墙的对应关系如下：

表6 思科防火墙OpenStack资源映射表

|  |  |  |  |
| --- | --- | --- | --- |
| ＃ | **OpenStack抽象资源** | **思科ASA防火墙对应资源** | **备注** |
| 1 | Firewall | Security context | OpenStack中firewall的创建在ASA中对应生成security context，同时生成internal和external的三层子接口并加入security context来做租户隔离。 |
| 2 | Policy | Access list |  |
| 3 | Rule | Access entry |  |

FWaaS Plugin将OpenStack中虚拟防火墙资源通过RPC的方式发送给ASA agent，一个ASA agent可以管控一台ASA设备、HA模式ASA集群或者Cluster模式ASA集群，同时ASA agent的分布式部署方式使得ASA设备的横向扩展能力得到提升，通过FWaaS Plugin中的调度算法，可将OpenStack中虚拟防火墙资源合理的分配到不同的ASA设备当中。

（4）网络资源与OpenStack映射模型

云管平台上层支持多个金融机构，每个金融机构是一个租户。每一个租户在OpenStack里对应一个项目，包涵多个逻辑云网分区和一个RI组成的隔离资源区。单个租户的每一个逻辑云网分区对应一个物理云网分区，每个物理云网分区支持多个租户的逻辑云网分区。

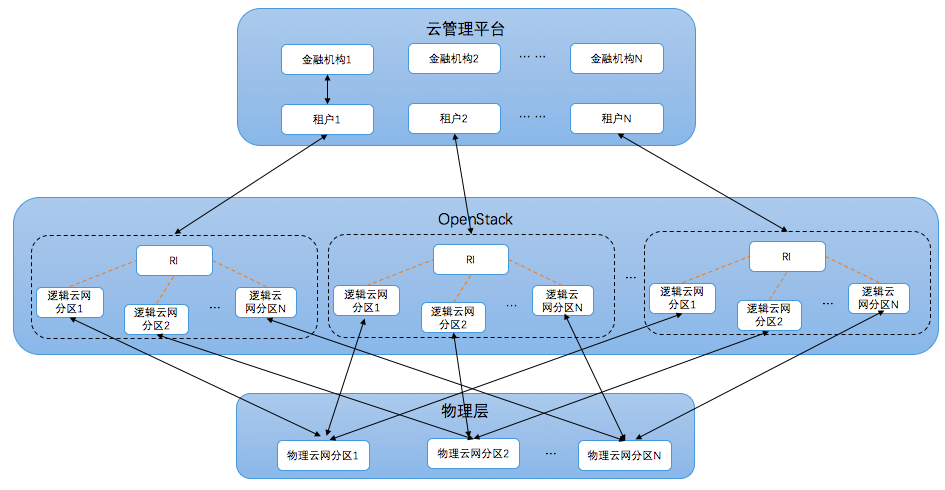


图11 多租户云网分区逻辑与物理资源映射关系图

在和ACI集成中，一个逻辑云网分区对应ACI中的一个租户概念，一个ACI租户含一个VRF，一个VRF内虚拟网络的流量全通。

在和AC集成中，一个逻辑云网分区对应AC中的一个VPC概念，一个VPC含一个VRF，一个VRF内虚拟网络的流量全通。

（四）效果展示

原型平台基于多租户能力，创建了中国银联与上海银行两个金融机构租户，两个租户的网络地址完全隔离复用，每个租户横跨华为与思科的两个云网分区资源，且共同复用所有硬件资源，通过核心交换网络进行数据互通。如下图在极端情况下，两个机构租户的虚拟机资源的部署与地址规划与开通完全一致



图12 多租户网络地址完全隔离复用

图13展示了原型平台金融机构租户管理员的管理服务界面，原型平台实现了云数据中心虚拟路由、负载均衡、防火墙网络资源以及相关网络安全配置的自动化开通能力与统一视图展示。

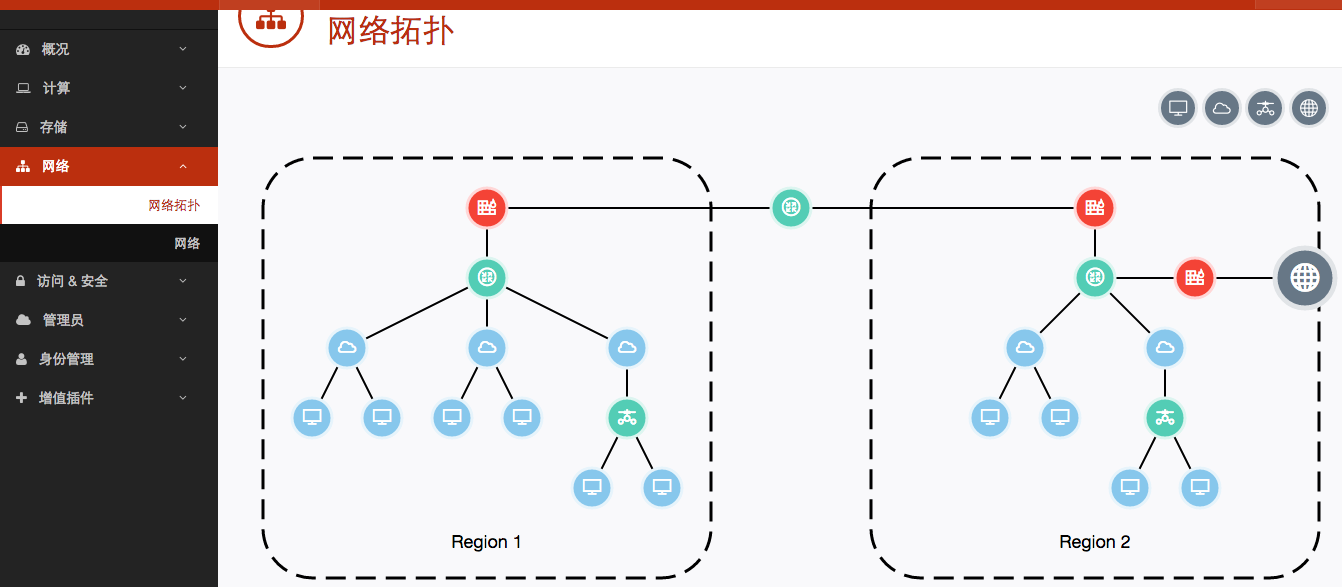


图13 租户管理服务界面展示的跨区组网视图

（五）实践中的问题识别与缺陷

基于当前银联生产技术的选型以及开放的研究角度，我们基于OpenStack开源技术进行了研究实现，在实现过程中不断汇总梳理了相应遇到的问题，一些影响核心应用的问题我们进行了个别优化解决，一些问题仍然有待解决，我们计划提交社区优化，具体如下：

（1）二/三层网络模型

* 三层模型不支持双出口

现有路由器模型仅支持一个去往互联网的External出口，模型不支持设置双出口，但金融机构DMZ区的往往需要两个出口，一个去往内网、一个去往外联网或互联网。

（2）防火墙模型

* 地址及服务对象定义方式有限

仅支持IP或网段，不支持IP范围、网段范围等，无法将多个地址对象组合成为一个地址组使用。无法将多个服务对象组合成一个服务组使用。这些限制会导致策略数量急剧增多，降低防火墙效率，不利于维护。

* 无法针对特定服务设置连接超时时间

无法满足特定长连接应用的需求，导致应用异常。

* 无法针对特定服务设置应用层协议探测

传统防火墙支持的ALG功能，动态开放端口等，在遇到非标端口时需进行设置（例如FTP协议使用了2121端口情况），但在防火墙模型中无此概念。

* 无法针对特定策略设置有效时间
* 无法基于防火墙实现地址转换

（3）负载均衡模型

* 负载均衡部署模型受限

现持单臂有负载均衡模型仅支模式，不支持双臂、多臂等。

* 无法设置连接超时时间

无法满足特定长连接应用的需求，导致应用异常。

* 无法设置会话保持设置超时时间

无法满足特定长连接应用的需求，导致应用异常。

* 支持算法较少

Listener支持类型较少、支持会话保持方法较少、支持负载均衡算法较少、支持健康检查方法较少

 （4）其他方面

* 部分网络关键组件缺少模型

如：IPS、DDOS网络安全、链路负载均衡等。

同时，我们通过研究后，我们也认为SDN Fabric控制器以及其他网络设备的API能力，或其提供的管理软件驱动可以进一步加强，以便可以在实现金融网络SDN能力时，可以更方便的获取相应细节参数以及加强管理的精细化力度。

1. 总结与展望

经过上述研究与实践，中国银联与上海银行的联合研究团队认为SDN技术的应用将是未来金融数据中心网络的发展趋势，当前技术积累，即未来基于SDN的下一代金融云网络架构设计可以推动未来的生产逐步应用。同时我们也认为金融云建设是一项技术集成创新、产业协同创新的重大、复杂性高的系统工程工作，金融机构技术研发应立足于金融科技核心，聚焦于SDN等技术应用之金融机构的特色技术解决方案，注重产业合作创新。当前，我们有计划与期望筹建金融行业在云计算领域的联合研究工作组，横向凝聚金融机构的研究力量，纵向联合IT产业各方，积极影响OpenStack等开源社区研发方向，共同推动金融云关键技术的突破与应用，提高金融云科技技术的普适性与标准化，非常欢迎大家，尤其是金融机构的合作伙伴能够一起参与我们发起的联合研究工作中，并多给予宝贵的指导意见，让金融云技术在世界范围内联网通用。

如何联系我们：请关注电子商务与电子支付国家工程实验室微信公众号



**作者介绍：**

祖立军，毕业于同济大学信号与信息处理专业，工学硕士，就职于中国银联电子支付研究院、电子商务与电子支付国家工程实验室，中国银联技术委员会专家，同济大学客座教师，长期从事金融信息工程领域研究工作，专注于金融端云一体化信系统建设。负责建成中国银联云计算平台，2011年提出OpenStack开源云软件的技术路线，并在生产大规模应用，参与国家云计算示范工程项目，现主持上海市科委课题“金融行业云关键技术研究及应用”研究,对金融企业云计算应用具有深刻理解，关注软件定义网络、软件定义存储、云间互联、智能云汽车等前瞻性技术。曾获国家科技进步二等奖1次，上海市科学技术一等奖1次，银行科技发展一等奖1次，2015年上海市软件行业标兵，2017年度上海市青年科技英才,累计申请或联合他人申请国内外专利18项，其中国内授权专利2项，国际授权专利2项，累计发表论文18篇，其中SCI检索2篇，EI检索6篇。

马永祥，毕业于上海大学通讯工程专业，工学学士，先后就职于工商银行数据中心（上海）、上海农商银行信息科技部、上海银行信息技术部，网络通讯领域技术专家，长期从事银行业网络技术研究、设计与实践，对于银行业数据中心网络规划有着丰富经验，现担任上海银行数据中心网络通讯部主管。曾负责多家大型银行数据中心网络系统规划、改造与建设工作，2009年-2011年参加工商银行数据中心（上海）园区扩建网络建设项目，实现工行网络架构优化升级，2011年-2013年牵头上海农商银行新一代银行系统建设网络集成项目，完成网络架构五年规划、张江数据中心投产、全行网络优化改造等工作。2013年-2017年牵头上海银行张江数据中心网络建设项目，完成网络两地三中心架构规划、张江数据中心网络建设及投产、应用系统迁移、网络改造等工作。

袁航，毕业于同济大学系统工程专业，工学硕士，现就职于中国银联电子支付研究院、电子商务与电子支付国家工程实验室，研究员。现负责中国银联创新研究环境的研发和建设、金融SDN评测标准（上海银行、复旦大学、上海宽带中心、思科、华为、华三、博科等18家单位，中国通信标准协会标准、中国银联标准技术指引）的制订等工作。关注于SDN软件定义网络、跨数据中心管理等前沿性技术，在OVS等网络开源软件在金融数据中心应用有深入研究。

王明辉，2010年开始就职于上海银行信息技术部，网络技术专家，上海银行科技项目技术方案评审小组成员，拥有CCIE（RS）证书，专注于金融机构两地三中心数据中心网络架构建设。曾参与上海银行张江数据中心网络架构设计和建设，配合完成张江数据中心的投产、应用系统迁移等重要工作。现牵头负责上海银行同城数据中心和异地灾备数据中心网络建设项目。2016年完成并行内发表了一篇《软件定义网络（SDN）技术研究》的课题研究论文，对基于IaaS云架构模型有较深刻的理解。关注软件定义网络、未来云数据中心架构、跨数据中心多租户运维管理等前沿性技术。

周雍恺，毕业于上海交通大学，信息安全专业,电子商务与电子支付国家工程实验室进行博士后研究，研究方向为SDN金融应用及其安全。在博士后期间，提出面向金融云的软件定义网络（SDN）安全研究理论与框架，正在牵头推动中国银联面向SDN网络的下一代云网监控系统的生产应用工作。

金斯，毕业于上海海事大学网络工程专业，拥有CCIE（RS）证书，长期从事银行业数据中心的建设运维工作，致力于金融行业云的研究。2012年至2013年就职于上海华讯网络系统有限公司，参与农商行新一代数据中心的建设迁移项目，完成了多个核心区域的迁移手册编写及实施。2014年就职于上海银行信息技术部，负责数据中心的网络运维及技术方案审核，曾牵头完成上海银行原主备数据中心多个核心区域的改造迁移项目。2016年开始参与SDN的课题研究，与同事共同完成了《软件定义网络（SDN）技术研究》课题研究论文，获得上海银行2016年课题研究二等奖。