



基于 SPICE 开源协议的云桌面技术架构研究

石屹嵘, 龚德志

(中国电信股份有限公司上海研究院 上海 200122)

摘要: 分析了云桌面特点、应用场景和行业主流实现协议, 结合实验室测试结果, 对主流协议进行性能对比分析。分析云桌面实现功能架构和编程架构, 从桌面绘图、接口调用流程和数据通道等方面研究开源 SPICE 技术架构特征, 对协议中需要重点关注的技术点进行阐述, 同时对 SPICE 开源协议应用前景进行展望和分析。

关键词: 开源; 云桌面架构; SPICE

doi: 10.3969/j.issn.1000-0801.2013.08.028

Research on Technical Architecture on the SPICE of Open Source VDI

Shi Yirong, Gong Dezhi

(Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200122, China)

Abstract: The features and scenarios and agreement of VDI were stated, performance of agreement base testing, and the functional architecture and programming architecture base desktop and interface calls and data channel of the SPICE were analyzed. The important point of technology and the prospect of SPICE were proposed.

Key words: open source, virtual desktop infrastructure, simple protocol for independent computing enviroment

1 引言

云桌面(virtual desktop infrastructure, VDI)技术是一种将用户数据、应用、操作系统等资源进行虚拟化和抽象, 实现多层次间的松耦合, 为用户提供安全、灵活的桌面环境的云计算技术。云桌面是服务器虚拟化在桌面系统的一种部署形式, 目的是方便资源动态调度、桌面管理和用户认证。云桌面给最终用户的体验和传统物理 PC 机桌面是一致的。

随着服务器虚拟化技术的发展、硬件设备性能的增强、网络条件的不断优化, 云桌面技术在大型企业客户, 尤其是银行、电信运营商中得到了越来越广泛的认可。云桌面具备以下特点。

- 计算、存储资源集中化: 将传统的本地 PC 的处

理能力(包括 CPU 和硬盘)集中到数据中心, 办公个人终端变成 TC(瘦客户机), 不需要强的处理能力和存储能力。

- 计算、存储资源共享化: 数据中心给每个办公终端提供虚拟化的“桌面”, 每个终端所使用的后端计算资源都是共享的。
 - 云数据中心统一调度和管理: 基于云计算技术的统一管理平台, 实现对资源的“按需分配”管理。
- 相对于传统的 PC, 云桌面具有以下价值。
- 接入便捷性: 只要有一个云桌面客户端, 并且具备一定的网络条件, 就可以在不同的地方访问数据中心的云桌面, 使用内部网络应用。
 - 可管理性提高: 云桌面都集中部署在数据中心。通过集中化管理, 维护人员可以维护更多的云桌面。

- 安全性提高:云桌面通过集中管控,所有的用户数据都保存在安全等级高的数据中心,且通过加密的 VDI 协议进行传输,可以大大提高系统的安全性。
- 节能减排:云桌面通过虚拟化技术可以做到资源共享、错峰填谷,且终端能耗远低于 PC 能耗,相对于传统的 PC,云桌面更具有环保性。
- 成本降低:如果使用大量云桌面替代传统 PC 桌面,长远来看能降低企业投资成本。

2 主要应用场景

云桌面技术在企业内部的应用具备一定的适用性,目前的传输协议和网络条件给云桌面的应用带来了一些局限性。下列应用场景短期不适合运行在云桌面环境中:

- 需要大量视频解析和渲染的环境,如在云桌面中播放高清视频会降低用户体验;
- 网络带宽有限的环境,云桌面对网络带宽和稳定性有一定的要求,2 Mbit/s 以下的网络会降低用户体验。

经过测试和实践,在以下 4 种应用场景中应用云桌面技术,可以体现云桌面的价值。

(1) 办公桌面

办公环境的特征:地域分布广泛,终端数量庞大,办公地点固定,办公应用相对简单。

办公桌面应用云桌面的价值在于:大规模使用云桌面,可以降低投资成本;采用桌面虚拟化可以进行集中管理,提高安全性和管理效率;推广便捷。

(2) 营业厅

营业厅环境的特征:地域分散,现场人员集中,业务连续性要求高。

营业厅应用云桌面的价值在于:桌面集中管理,降低运维成本;缩小主机体积,提高营业厅现场环境利用率;减少营业厅现场设备功耗,实现节能减排;云计算数据中心的高可用性,能保证业务连续性。

(3) 呼叫座席

呼叫座席的特征:人员集中,业务连续性要求高;应用统一;除音频之外,业务系统以查询、点击、字符输入为主。

呼叫座席应用云桌面的价值在于:可以降低投资成本;部署快捷;减少呼叫中心现场设备功耗,实现节能减排;云计算数据中心的高可用性,能保证业务连续性。

(4) 网管维护

网管维护桌面应用主要特点:厂商人员行为需受控;可根据用户应用调整资源规格;用户开发应用软件种类众多;用户应用操作层面日志记录和审计;设端口使用管理。

网管维护应用云桌面的价值在于:可以支持各种终端接入,实现远程维护和监控,有利于企业发挥维护专家优势;提高安全审计功能。

3 相关技术

云桌面涉及多种云计算相关技术,其中最重要的是两种技术:一种是服务器虚拟化技术,另一种是桌面传输和展现技术。

(1) 服务器虚拟化技术

服务器虚拟化也称系统虚拟化,把一台物理计算机虚拟化成一台或多台虚拟计算机,各虚拟机间通过虚拟机监控器(virtual machine monitor, VMM)的虚拟化层共享 CPU、网络、内存、硬盘等物理资源,每台虚拟机都有独立的运行环境。虚拟机可以看作对物理机的一种高效隔离复制,要求同质、高效和资源受控。同质,说明虚拟机的运行环境与物理机的环境本质上是相同的;高效,指虚拟机中运行的软件需要具有接近在物理机上运行的性能;资源受控,指 VMM 对系统资源具有完全的控制能力和管理权限。一般来说,虚拟环境由 3 个部分组成:硬件、VMM 和虚拟机。VMM 取代了操作系统的位置,管理着真实的硬件。

目前云桌面中采用的服务器虚拟化技术主要有:微软公司的 Hyper-V、Citrix(思杰)公司的 Xen Server、VMware 公司的 VMware vSphere 和 Red Hat 公司的 KVM。

(2) 桌面传输和展现技术

桌面传输和展现技术主要是一种将远程云桌面和音频信息,传输至接入终端,在接入终端上进行展现,并和接入终端外设进行交互的技术。在云桌面中,桌面传输和展现技术的选择和服务器虚拟化技术之间的关系是密不可分的。通常情况下,选择了桌面传输和展现技术,也就决定了对应的服务器虚拟化技术。

目前的技术实现方式和协议主要有以下 4 种:

- 微软公司,桌面传输和展现基于 RDP。
- Citrix 公司,桌面传输和展现基于 ICA 协议。
- VMware 公司,桌面传输和展现基于 PCoIP。



- Red Hat 公司, 桌面传输和展现基于 SPICE (simple protocol for independent computing environment) 协议。

前 3 种实现方式采用的均为封闭协议, 软件授权价格非常贵。云计算运营商采用这 3 种实现技术开发云桌面产品将面临很大的成本压力。经过测算, 在整个建设云桌面的成本中, 50% 左右为软件成本。并且因为协议封闭, 云计算运营商对云桌面产品的二次开发变得非常困难。

第 4 种实现方式中, KVM 服务器虚拟化技术和 SPICE 远程桌面传输和展现协议是开源的。目前越来越多的国内云桌面开发商选择基于该方式进行云桌面产品开发。本文就协议传输性能、功能模型、编程架构, 结合笔者已经实现的产品原型进行分析。

4 主流实现技术性能对比

选择云桌面协议时, 除了考虑该协议是否开源, 能进行定制和开发外, 另外一个重要指标是该协议的传输性能。传输性能好的协议网络负载低, 数据压缩比率高, 用户在使用云桌面产品时, 感知比较好。

为比较 4 种协议的传输性能, 在实验环境中, 对 4 种协议进行了多维度的测试, 其中最重要的一项测试是视频传输性能。

测试环境介绍如下:

- 一台 HP DL380 (2 路 4 核 2.27 GHz CPU, 32 GB 内存, 吉比特网络) 服务器用于安装云桌面相应的服务器虚拟化软件, 承载云桌面以进行性能测试。
- 一台 HP DL380 (2 路 4 核 2.27 GHz CPU, 32 GB 内存, 吉比特网络) 服务器用于安装云桌面管理平台, 实现云桌面和用户的管理。
- 10 台 PC 机 (P4/2.2 GHz CPU, 1 GB 内存, 百兆网络) 安装 Windows XP Professional 操作系统和云桌面客户端, 接入云桌面。

测试目的: 测试云桌面传输和展现协议对网络资源和接入终端 CPU 资源的占用情况。

测试方法: 在云桌面环境中, 开启 1 个云桌面, 关闭其他云桌面。通过 1 台 PC 机, 安装接入客户端, 接入云桌面, 播放一段高清视频。监控云桌面服务器网络资源利用率和接入终端 CPU 利用率。高清视频片长 2.5 min, 文件大小为 47.8 MB。

测试结果: ICA 协议和 SPICE 协议对网络资源、接入终端 CPU 资源占用最小, 具体见表 1。

从表 1 可以看出, 开源 SPICE 协议和 ICA 协议的云桌面产品性能差异不大, 比基于 RDP、PCoIP 的云桌面产品性能好, 所以基于开源 SPICE 协议进行开发的云桌面产品在性能上有较大的优势。

5 平台功能模型

基于开源 SPICE 协议开发云桌面产品, 可以基于以下功能模型实现产品开发。云桌面功能模型如图 1 所示。

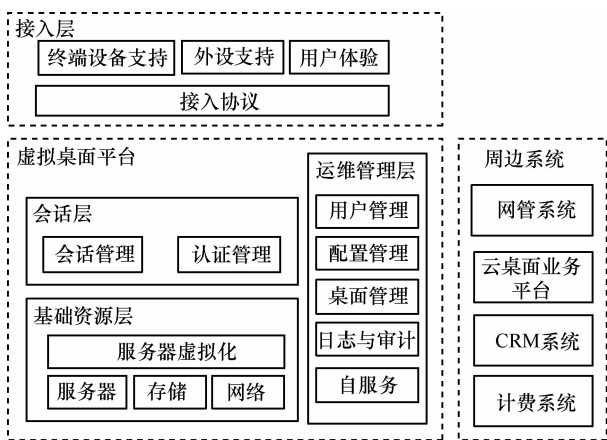


图 1 云桌面功能模型

模型各部分的功能概述如下。

(1) 接入层

接入层是实现用户终端接入云桌面系统的功能层, 其

表 1 测试结果

测试指标	RDP	ICA	PCoIP	SPICE
接收网络流量 (byte)	478 123 696	158 850 231	179 624 322	165 631 318
发送网络流量 (byte)	11 920 757	4 747 019	660 230	4 291 760
平均接收速度 (Mbit/s)	24.442	8.364	9.929	8.885
平均发送速度 (Mbit/s)	0.609	0.25	0.037	0.23
终端 CPU 占用情况	35%	30%	80%	30%
播放效果	流畅	流畅	流畅	流畅

核心功能为用户终端接入管理,主要包括终端设备支持、接入协议、外设以及用户体验等。

- 终端设备支持指用户可以通过各种类型的终端接入云桌面,包括PC(台式机或笔记本电脑)、瘦客户机设备、移动终端设备等。
- 接入协议指接入层通过SPICE协议接入云桌面。
- 外设支持指云桌面系统对连接在用户终端上的计算机外设提供支持,确保外设的正常使用,以满足业务需求,包括串口、并口和USB等不同类型的外设接口,并对这些端口提供良好的重定向能力。
- 用户体验指用户远程访问云桌面时,桌面展示和操作使用习惯应该与使用本地操作系统一致。

(2) 会话层

会话层是实现用户终端远程连接云桌面系统的访问控制和会话生命周期管理的功能层,包括认证管理和会话管理。

- 认证管理是对用户终端接入云桌面系统进行认证。用户完成一次登录认证后,在一定时间期限内无需多次重复登录,即可直接访问云桌面。
- 会话管理是对用户远程访问桌面的整个会话过程进行管理,包括会话连接管理、会话功能控制和会话访问控制等,是云桌面管理平台的核心功能,可通过直接管理会话或者设定相关的会话管理策略实现。

(3) 基础资源层

基础资源层是对服务器端提供的桌面或应用资源进行管理的功能层,包括物理服务器、虚拟机以及在上面运行的桌面统一管理。服务器虚拟化即第3节提到的服务器虚拟化技术,在开发过程中一般无需对服务器虚拟化的实现方式进行二次开发。

(4) 运维管理层

运维管理层是支撑云桌面系统正常运行的相关辅助管理能,包括用户管理、配置管理、桌面资源管理、日志与审计管理和自服务等。

- 用户管理是对登录云桌面系统的终端用户进行管理,包括用户权限、用户数据等管理功能。云桌面系统的多个用户能够组成用户组,进行统一管理。
- 配置管理是在云桌面系统安装部署、

运行期间,对相关软硬件的属性进行采集、存储、跟踪和比对和修改等操作。

- 桌面资源管理是对云桌面的功能进行管理,包括桌面部署、发布、启动、使用、回收、销毁等。
- 日志与审计管理是指对全部用户操作及系统事件进行记录,以便跟踪、分析系统全部运行状态,并为审计提供数据支持。
- 普通用户可以通过自服务界面进行云桌面的启动、关闭、配置调整申请。

(5) 周边系统接口

周边系统接口包括云桌面运维管理平台与网管系统、云桌面业务管理平台、CRM系统和计费系统的接口。

6 SPICE 协议编程架构

SPICE 主要包括 SPICE 协议、SPICE 服务器和 SPICE 客户机 3 部分。SPICE 相关组件包括 QXL 设备以及用户机 QXL 驱动。

6.1 SPICE 协议绘图流程

SPICE 协议的基本构架以及使用带 SPICE 库的 QEMU(模拟处理器)时,图形命令的 guest 至 client 的数据流程如图 2 所示,绘图过程如下。

- 当接入客户端的应用程序向操作系统的图像引擎(X或GDI)发出图形渲染请求时,就启动了SPICE图形命令流程。
- 图像引擎将命令传递给QXL驱动器,QXL驱动器将此OS命令转换为QXL命令,再将其加入存在于QEMU设备内存中的命令环内。
- SPICE库从命令环中取出命令并将其加入命令树中,从而图形命令树中包括控制输出内容的命令集。
- SPICE库会将此命令集中,将其他命令覆盖的命令剔除,再将优化后的命令传输给客户端。同时命令树还用于对视频数据流的侦测。

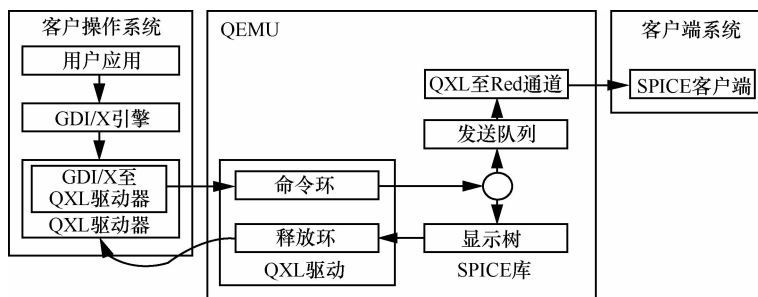


图2 SPICE 协议基本架构



- SPICE 库同时运行一个命令队列以备发往客户端,更新输出,从命令集中取出并传递给客户端的命令将会被转换为 SPICE 协议消息。
- 从命令树中移除的命令也从发送队列中移除,不再为 SPICE 库所用的命令将会被加入 QEMU 设备的释放环中,此环将被 QXL 驱动器用来释放命令资源。
- 客户端将执行收到的图形命令,以更新显示。

6.2 代理调用流程

SPICE 代理(agent)是运行于用户机内的软件模块,被 SPICE 服务器以及客户端用来执行诸如配置显示参数等本地环境下的任务。图 3 揭示了二者通过虚拟设备接口端口和用户机驱动程序与代理交互的过程。

相关消息的来源有客户端(如配置用户机显示)、服务器(如鼠标移动)以及代理(如配置应答)。

驱动器通过其 I/O 环与设备通信。由客户端及服务器产生的消息会被写入服务器的写队列,再写入设备的输出环中,消息将从设备的输入环读入服务器的读缓存,端口将决定消息由服务器处理或发往客户端。

6.3 SPICE 客户端

SPICE 客户端如图 4 所示。通用接口即 Platform 类,其定义了许多诸如定时器和光标操作等底层服务。Application(应用类)为主类,其包含并控制客户端、显示器及屏幕,处理一般应用任务,如解析命令行参数、运行主消息循环、处理事件(连接、断开、错误等)、将鼠标事件重定向至输入处理和切换全屏模式等。

客户端与服务器通过通道进行通信。每个通道类都被设定为特定的数据类型,并使用特定的 TCP socket,且可选择是否通过 SSL 加密。

RedClient 为主通道,它拥有并掌控其他所有实体通道(通过 factory 创建通道、连接、断开等),并处理通道的控制、配置及迁移(通过 Migrate 类)等任务。

可用通道介绍如下:

- 主通道(main),由 RedClient 实现的主通道;
- 显示通道(display channel),处理图形命令、图像以及视频数据流;
- 输入通道(inputs channel),用于鼠标键盘输入;

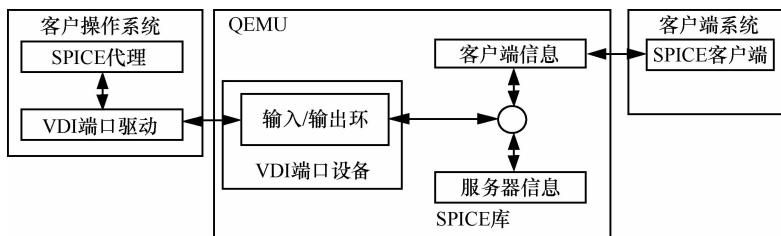


图 3 SPICE 代理调用流程

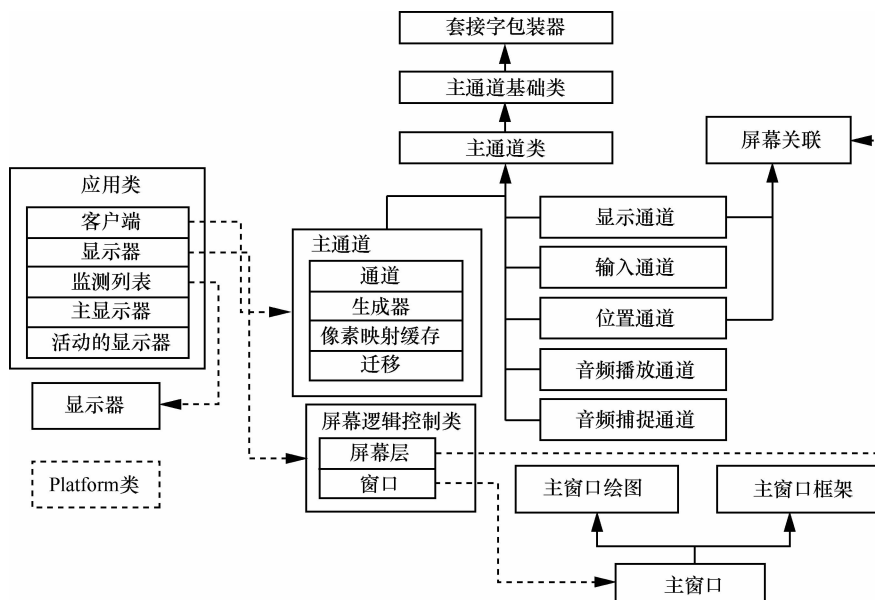


图 4 SPICE 客户端

- 位置通道(cursor channel),指示设备的位置、可视性和光标形状;
- 音频播放通道(playback channel),指示来自服务器待由客户端播放的音频;
- 音频捕捉频道(record channel),指示客户端捕捉的音频。

7 结束语

SPICE 协议实现了通用接口的定义,可以直接对接口进行调用,而将平台相关的实现置于对等目录中。编程过程中,较容易实现屏幕绘图和通道信息的传输。SPICE 协议已经显现了 6 个通道的定义,基本满足云桌面远程连接和桌面展现的需求,而且新通道的定义也较容易实现,经过后期开发,也能实现应用程序数据的传输。

目前笔者已经实现基于 SPICE 协议的云桌面原型系统开发,实现的功能包括多终端统一接入、云桌面用户和桌面管理以及自服务门户,具体介绍如下。

- 多终端接入功能,包括支持 PC、瘦终端、Android 终端、iOS 终端接入云桌面。
- 云桌面用户管理功能,包括用户创建、编辑、分组等。
- 桌面管理功能,包括桌面的创建、修改、克隆、删除和分配等。
- 自服务门户,用户可以通过自服务门户提交性能扩容申请,包括对云桌面进行启动、关闭、重启等。

该云桌面原型系统在公司内部进行了一年左右的试点,效果较好,平台未出现性能问题和功能故障。

总的来看,基于 SPICE 开源协议,在功能上,能实现行

业内优秀的云桌面产品的功能。开源 SPICE 协议的云桌面将是未来云桌面领域的一匹“黑马”,为国内云桌面产品的应用推广推波助澜。

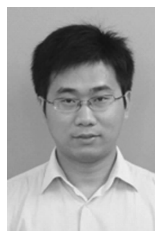
参考文献

- 1 龚德志, 闻剑峰. 虚拟化技术在电信服务器资源整合中的应用研究. 电信科学, 2009, 25(9)
- 2 石屹嵘, 段勇. 云计算在电信 IT 领域的应用探讨. 电信科学, 2009, 25(9)
- 3 闻剑峰, 龚德志. 虚拟化技术在电信灾难恢复计划中的应用研究. 电信科学, 2009, 25(9)
- 4 成静静. 基于虚拟化的云桌面技术方案研究与设计. 广东通信技术, 2011, 31(6)

[作者简介]



石屹嵘,男,中国电信股份有限公司上海研究院高级工程师、信息技术部主任工程师,长期从事系统架构、云计算、系统审计和信息安全等方面的研究工作。



龚德志,男,中国电信股份有限公司上海研究院工程师、中国电信企业信息化验证实验室主管,主要研究方向为云计算、大数据、信息系统评测和容灾。

(收稿日期:2013-03-05)

(上接第 161 页)

查杀。本技术方案实施后,将为移动通信网络提供优质的风险评估、安全防护符合性评测和安全咨询等专业服务,在保障移动通信网络的安全稳定运行、人民群众安全通信和减少国家经济损失方面具有重要意义。

参考文献

- 1 李钧. 移动互联网的安全之思. 网络与信息, 2011(10):61~63
- 2 <http://www.cnnic.net.cn/dtygg/dtgg/201207/W020120719405405832029.pdf>
- 3 王勇斌. 移动互联网网络安全探析. 现代电信科技, 2008, 39(8):

28~30

- 4 <http://www.cert.org.cn/publish/main/upload/File/201208282mobile.pdf>
- 5 潘娟, 史德年, 马鑫等. 移动互联网形势下智能终端安全研究. 移动通信, 2012, 3(5): 48~51

[作者简介]

李俊,男,中国移动通信集团江苏有限公司网络部工程师、部门副总经理(资深),主要研究方向为通信网络网管支撑系统、网络安全与信息安全。

(收稿日期:2013-07-25)