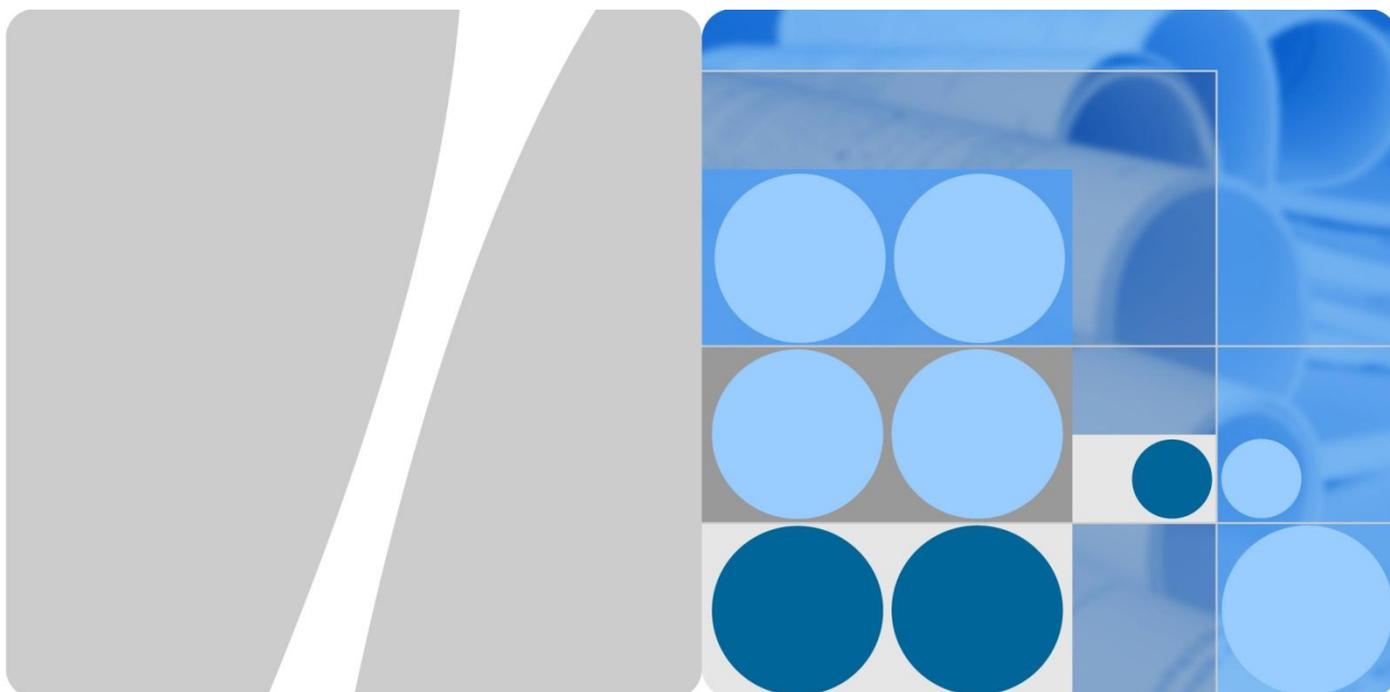


资料编码



ONE NET Campus 桌面云方案
V100R001C02
技术白皮书

文档版本 01
发布日期 2012-07-30

版权所有 © 华为技术有限公司 2012。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编： 518129

网址： <http://enterprise.huawei.com>

客户服务邮箱： ChinaEnterprise_TAC@huawei.com

客户服务电话： 4008302118

目 录

1 前言	1
1.1 当前各种类型桌面终端对比.....	1
1.2 桌面云方案提出.....	2
1.3 桌面云趋势.....	3
1.4 桌面云对网络质量要求.....	3
1.4.1 时延、抖动和丢包率要求.....	3
1.4.2 带宽要求.....	4
2 OA 集中办公技术介绍	5
2.1 概述.....	5
2.2 办公应用场景.....	6
2.2.1 终端接入场景.....	6
2.2.2 桌面操作/打印场景.....	7
2.2.3 电话/VOIP 业务场景.....	8
2.3 办公区网络设计.....	9
2.3.1 接入层设计.....	9
2.3.2 办公区汇聚/核心层设计.....	9
2.3.3 办公区网络规模和产品选型设计.....	10
2.4 数据中心网络设计.....	11
2.4.1 数据中心组网设计.....	11
2.4.2 数据中心网络规模和产品选型设计.....	12
2.4.3 数据中心流量模型设计.....	13
2.5 网络质量设计.....	16
2.5.1 网络质量指标要求.....	16
2.5.2 网络质量监控设计.....	18
2.5.3 QoS 设计.....	19
2.6 可靠性设计.....	20
2.6.1 网络设备可靠性设计.....	20
2.6.2 数据中心可靠性.....	21
3 城域营业厅技术介绍	22
3.1 概述.....	22

3.2 营业分厅组网设计	23
3.3 网络部署设计	23
3.3.1 城域自建 OSPF 多区域	23
3.3.2 城域自建 OSPF 单区域	24
3.3.3 租用 MPLS L3VPN	25
3.3.4 三种方式的对比	26
3.4 带宽设计	27
3.5 网络质量和监控设计	27
3.6 可靠性设计	28
3.7 产品选型	29
4 广域桌面云技术介绍	1
4.1 概述	1
4.1.1 典型组网	1
4.1.2 广域应用业务和性能分析	2
4.1.3 广域桌面云流量模型	3
4.2 带宽设计	4
4.3 网络质量设计	5
4.4 广域加速设计	6
4.5 性能路由设计	8

1 前言

1.1 当前各种类型桌面终端对比

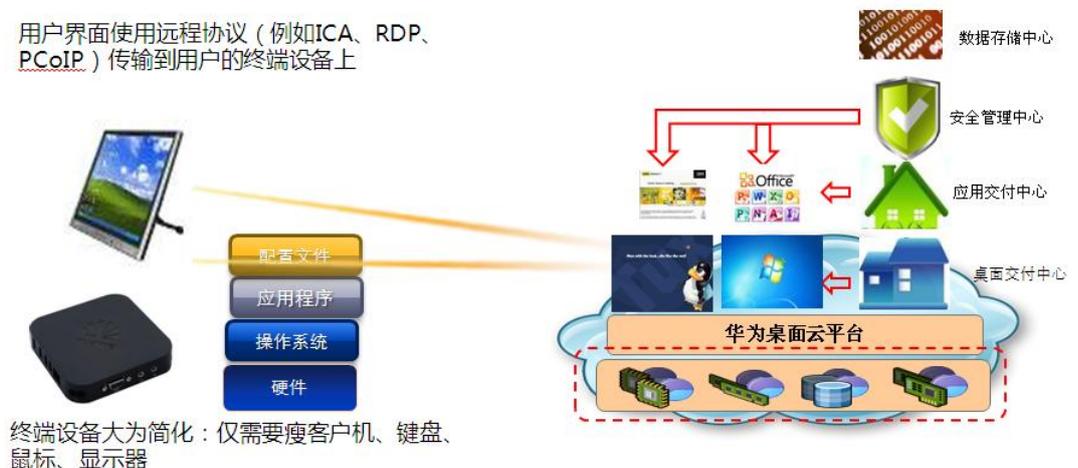
表1-1 当前各种类型桌面终端对比

终端类型	方案特点	优缺点分析
固定 IT 桌面	主机含带硬盘、内存和 CPU，与显示终端本地近距离连接	安全性差： 保存本地难以保证数据的安全，易丢失易泄露。数据通过网络传递易被截获。 资源耗费大： 一台桌面必须配备一台 PC，含带硬盘、CPU 和内存，资源利用不充分；每个客户端一个主机，带来高能耗、高排放。 接入不方便： 主机固定，用户只能固定场所办公，移动极为不便。 维护成本高： 每次软件、硬件故障或升级都需要到特定用户，耗费大量人力维护。
手提便携	主机和显示终端合为一体，便于携带	接入方便： 容易携带，随地接入进行办公，包括远程出差等
小型机拖终端	不同厂家采用专用显卡、硬盘等硬件	接入不方便： 各厂家的小型机相互之间难以兼容。
无盘工作站	用户只需一个显示终端，并含带内存和 CPU，硬盘统一集中后台存放	安全性良好： 保存数据中心，不易丢失泄露，但客户端掉电后数据就会全部丢失，而且数据通过网络会被截获。 资源耗费较小： 终端省了硬盘，但对于 CPU/内存与普通 PC 相当配置，不能动态共享，有一定耗电和硬件浪费。 体验效果一般： 高清视频播放和图片显示，需要通过一定带宽和低时延网络得以保障。

终端类型	方案特点	优缺点分析
桌面云	硬盘、内存、CPU 甚至网络、应用软件都在数据中心共享复用，用户仅需一台瘦身终端，无需主机	<p>安全性优：真实数据不经过网络难被截获；客户端掉电后整个会话重新接入数据不丢失。</p> <p>资源耗费最小：硬盘、内存、CPU 甚至网络、应用软件都可以共享，用户仅需一台瘦身终端，无需主机，省电无噪音。</p> <p>维护成本低：数据中心网管人员统一维护部署终端，可通过远程协助解决故障，大大降低维护成本</p> <p>接入最方便：用户可以随地接入桌面远程办公，无盘工作站只能在局域网内工作。</p> <p>体验效果一般：高清视频播放和图片显示需一定网络质量得以保障。</p>

1.2 桌面云方案提出

图1-1 桌面云方案示意图



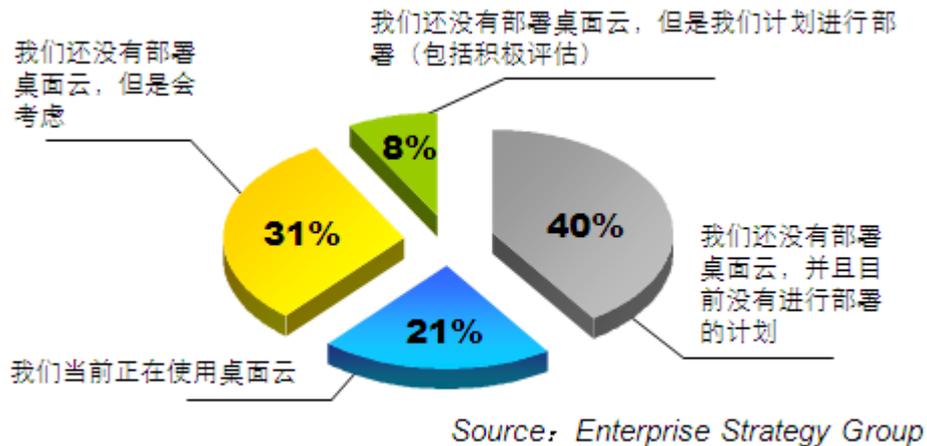
桌面云解决方案特点如下：

- 构建共享资源池，统一管理，可靠，可扩展
- 操作系统与硬件解耦，集中交付
- 应用程序与操作系统解耦，集中交付
- 数据与操作系统解耦，集中存储
- 构建多层次安全体系，分布式控制

1.3 桌面云趋势

Gartner 认为绝大多数 VDI 用户是从台式机用户迁移过来的。基于这个认识，Gartner 预测在 2014 年 VDI 将达 7 千万用户。云计算时代，桌面云已是大势所趋。传统桌面架构正在向桌面云架构迁移。

图1-2 桌面云发展趋势



全球52%的大型企业和48%的中型企业会计划采用桌面云服务。

目前桌面云具体应用如呼叫中心绿色座席，营业厅桌面云，OA 办公桌面云，高性能图形桌面云。按照距离主要划分为三类，OA 集中办公桌面云；城域营业厅桌面云；广域桌面云。

1.4 桌面云对网络质量要求

1.4.1 时延、抖动和丢包率要求

质量等级	体验效果	包丢失率	抖动(ms)	双向时延(ms)
良好	OA 体验同传统桌面无差异，标清播放有微弱滞后感	≤0.1%	≤5	≤50
一般	鼠标拖动有微弱滞后感，高标视图有卡顿感	≤1%	≤20	≤100
较差	鼠标拖动有轨迹，桌面显示有顿挫感	≤5%	≤60	≤400

1.4.2 带宽要求

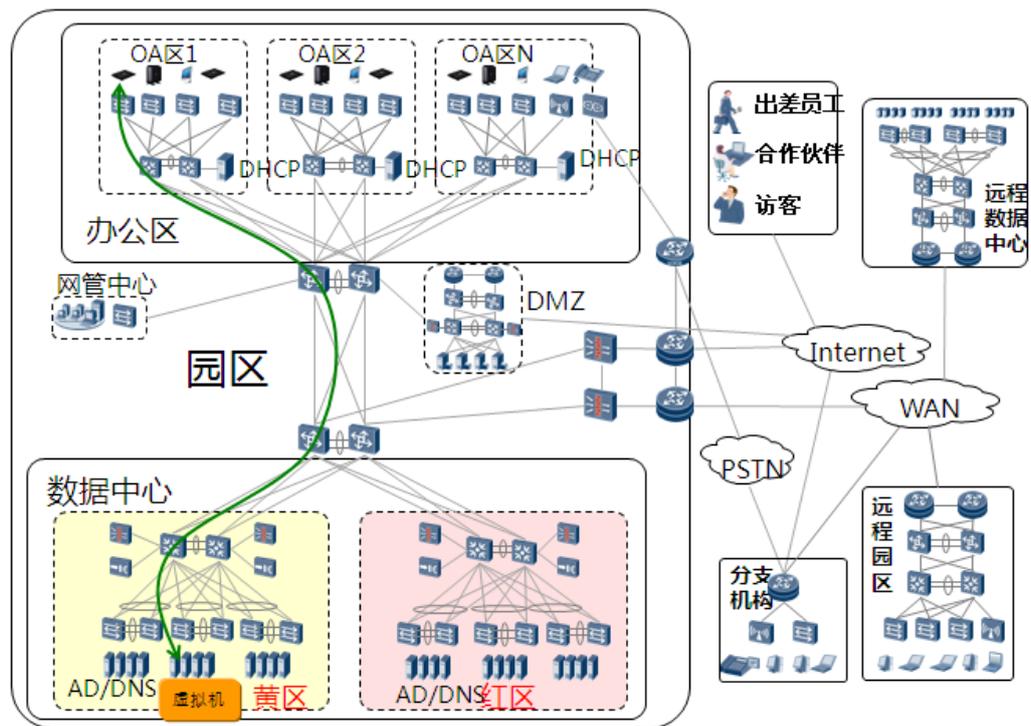
业务类型	带宽要求
Office OA 日常办公应用（Word/Excel/WWW 浏览）	占用 50~80Kbps
呼叫中心客服应用	100~150Kbps
PowerPoint/图片应用	占用 200~300Kbps
标清视频	占用 1~2Mbps

往往分配足够大带宽（一般 20M），避免拥堵现象造成的时延、抖动问题。

2 OA 集中办公技术介绍

2.1 概述

图2-1 OA 集中办公方案组网图

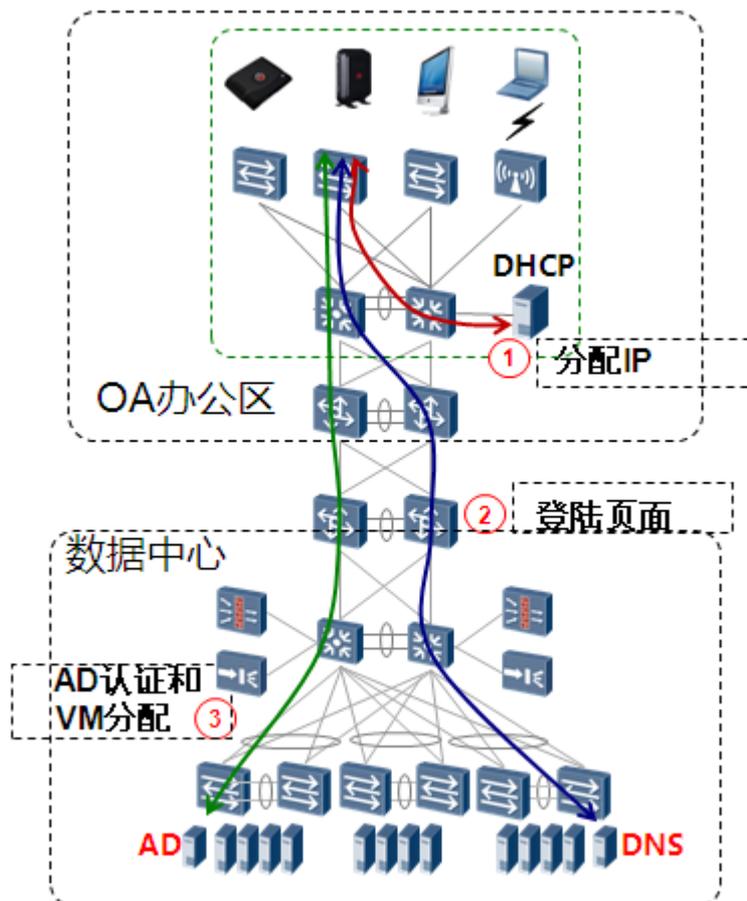


园区集中 OA 办公方案中，瘦终端通过园区网络和数据中心连接，距离 100 公里内。

2.2 办公应用场景

2.2.1 终端接入场景

图2-2 终端接入场景



终端接入过程如下：

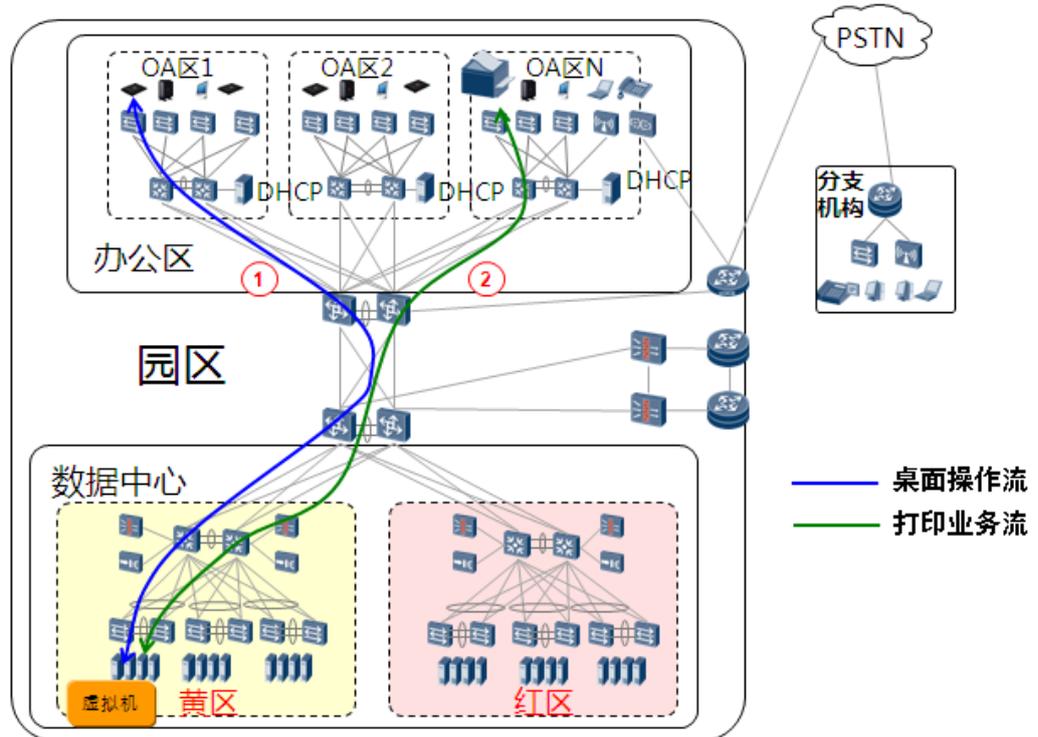
1. 终端从 DHCP 获取 IP 地址。
2. 访问 DNS 服务器解析获得域名 IP，并打开登陆页面。
3. 输入用户名/密码 AD 服务器认证。
4. AD 认证通过，云管理服务器分配 VM，并将 VM 服务器 IP 发给终端，建立 ICA 通道。

服务器部署位置如下：

- DHCP：部署在汇聚三层网关
- AD：部署在本地数据中心
- DNS：部署在本地或总部数据中心

2.2.2 桌面操作/打印场景

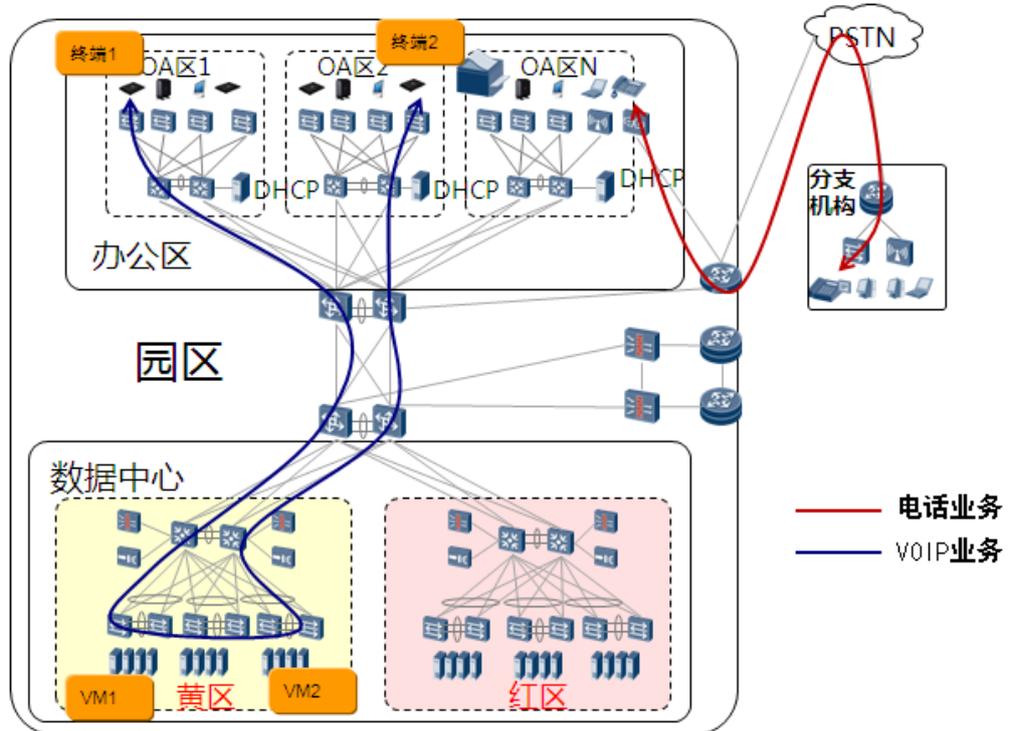
图2-3 桌面操作/打印场景



- 桌面操作业务流：键盘鼠标向数据中心虚拟机传递操作输入，虚拟机给终端 ICA 消息显示操作结果。
- 打印业务流：虚拟机 VM 向办公区打印机传输打印数据。

2.2.3 电话/VOIP 业务场景

图2-4 电话/VOIP 业务场景

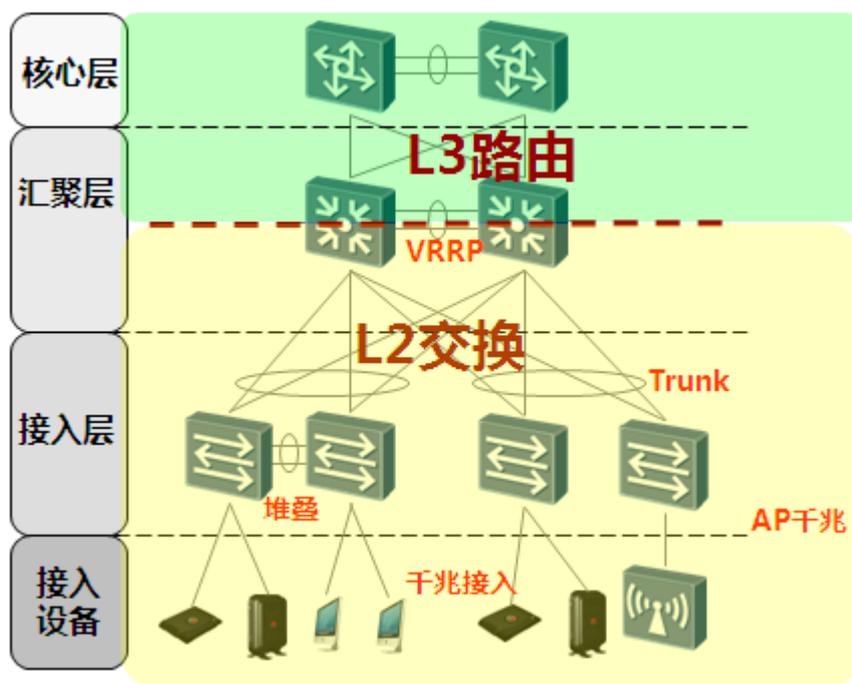


- 电话业务：通过 PSTN 园区办公和分支办公互联。
- VOIP 业务：语音由终端 1 话筒输入，到达自己的虚拟机 VM1，数据中心内部传输给 VM2，最后把语音传输给终端 2。

2.3 办公区网络设计

2.3.1 接入层设计

图2-5 接入层设计



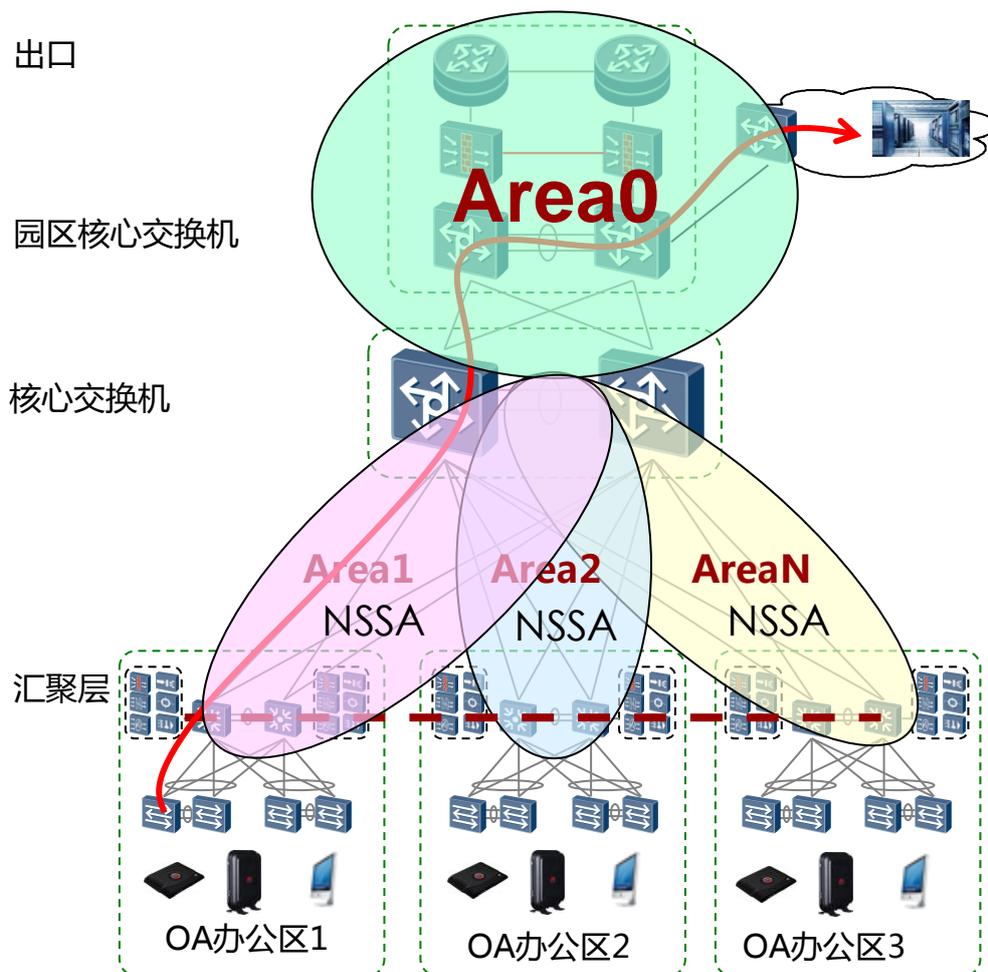
- 应用场景：办公区二层网络，承载键盘鼠标和 ICA 显示数据。
- 组网部署：终端接入 S5700 千兆接口，无线 AP 接入 S5700 千兆接口，S5700 堆叠实现二层交换，采用 Trunk 链路带宽复用，部门间不互访，无 VLAN 隔离汇聚层不堆叠选用 VRRP 网关。
- 客户价值：OA 用户千兆带宽接入，保证足够业务带宽和体验。

2.3.2 办公区汇聚/核心层设计

组网形式

办公区汇聚/核心层网络主要实现数据的汇聚和高速转发，通常是三层路由转发网络。在组网形式上，主要采用高性能的堆叠汇聚/核心交换机进行组网，并通过 XGE 链路或者 XGE 捆绑的 Eth-Trunk 链路，连接各办公接入区网络以及数据中心网络。

图2-6 办公区汇聚/核心层组网



路由规划

- 园区核心、数据中心核心交换机和出口路由器组成骨干区域（Area 0）。
- 每个OA办公区汇聚和核心交换机组网部署为不同的OSPF区域（Area 1、2……N）。
- 采用OSPF Stub 或者NSSA区域，限制外部LSA散播。
- 若分区数量少，建议全配置Area 0。
- 数据中心和园区核心交换机距离较远部署的话，可通过BGP连通。

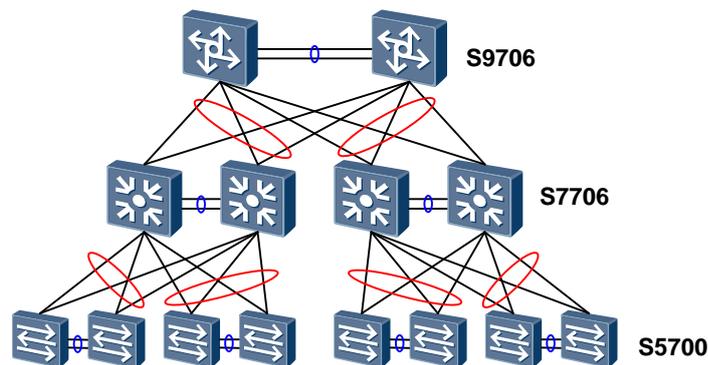
可靠性

- 通过硬件BFD实现10ms快速故障检测。
- 核心交换机采用NSR、GR协议平滑倒换保证桌面云流量无间断。
- 采用ISSU无损升级技术，设备升级过程中同时保证OA用户无缝体验。

2.3.3 办公区网络规模和产品选型设计

以下以5000桌面云用户（每用户20M带宽）为例，说明设备和链路的选型建议。

图2-7 办公区网络设备和链路选型



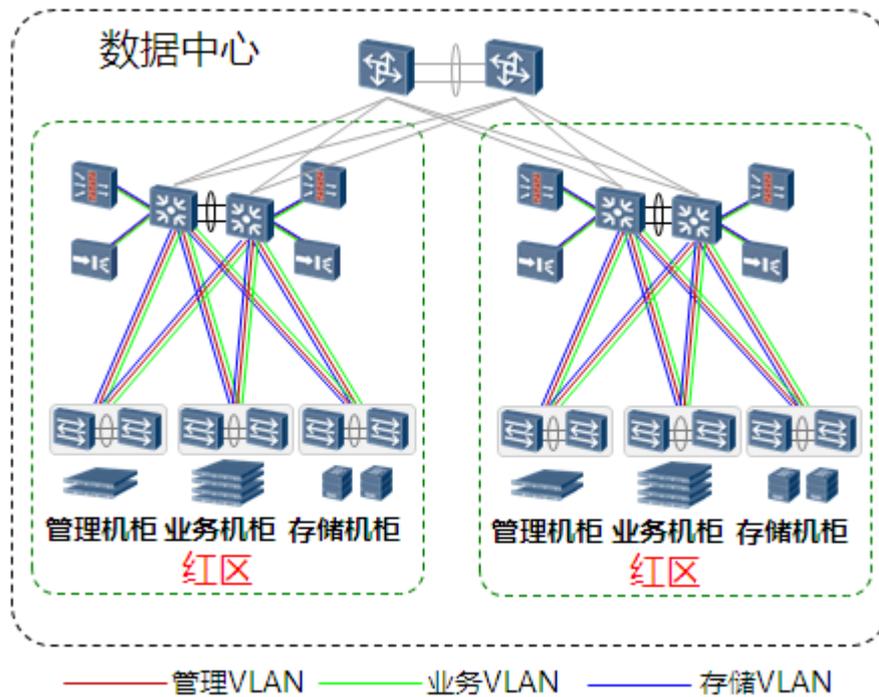
- 接入层
5000 用户规模，每桌面云用户需要 20M 带宽，共需预留 100GE 带宽。采用 S5700 配置 48GE（下行）+2*10GE（上行），2 台为一组。5000/（48*2）=53 组，共需要 106 台 S5700 设备。收敛比为：1：2.4。
- 汇聚层
S5700 共 212 接口上行连入汇聚层，采用 S7706 配置 6*12*10GE，212/（6*12）=3 台，2 组 4 台。212 接口连入接入层，64 接口上行接入核心层。收敛比为：64:212=1：3.3。
- 核心层
64 个 10GE 汇聚层 Trunk 接口连入核心层，需要 S9706 配置 3*16*10GE+4*40GE，2 台并为一组。4 个 40GE 接口连入数据中心核心层。4 个 10GE 接口连入园区出口。

2.4 数据中心网络设计

2.4.1 数据中心组网设计

OA 集中办公桌面云业务的数据中心的组网设计如图 2-8 所示。

图2-8 数据中心组网设计



在本组网中,物理机柜划分放置管理、业务和存储服务器,虚拟 VLAN 划分隔离管理、业务和存储网络平面。

- 业务网络：用来承载用户侧 TC 到 VM 的流量以及 VM 平常办公的流量。
- 管理网络：用来承载管理系统内部的流量。
- 存储网络：用来承载虚拟机到 IP SAN 存储的流量。

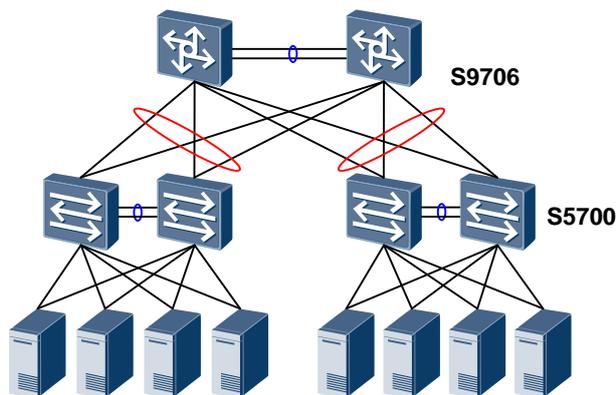
在管理和业务平面上,两层面数据流在全园区网络传输,两层面与存储层面通过 VLAN 隔离,通过防火墙过滤保证业务流安全,汇聚层作为 VRRP 网关,可部署 ME60 限制业务流带宽。

在存储平面上,存储数据流在只进行二层转发,主要用于服务器内部访问;通过 VLAN 与管理、业务平面隔离。

2.4.2 数据中心网络规模和产品选型设计

本节以服务器数量少于 1800 台的中小企业数据中心为例,说明数据中心网络的带宽设计,以及设备和链路的选型建议。

图2-9 数据中心网络设备和链路选型



- 接入层
1800 台服务器，每服务器双网卡接入，需要接入 3600 端口 GE。
在实际选型中，可选用 S5700 作为 TOR 交换机，下行 48 个 GE 口接入用户，上行 2 个 XGE 口接入汇聚交换机，每两台 S5700 为一组堆叠。
 $3600 / (48 * 2) = 38$ 组，共需 76 台 S5700，带宽收敛比为 1:2.4。
- 核心/汇聚层
接入层共有 $76 * 2 = 152$ 个 XGE 接口需连入核心/汇聚层。
因此核心/汇聚层可采用两台 S9706，每台配置 8 块 16*XGE 接口板，2 台并为一组，共提供 256*XGE 接入能力。152 个接口接入现有服务器，剩余 104 个可用来扩容。

表2-1 数据中心网络设备和链路选型表

网元	产品	数量	接口配置
核心/汇聚交换机	S9706	2 台	8*16*XGE
接入交换机	S5700	76 台	48GE（下行）+2*XGE（上行）

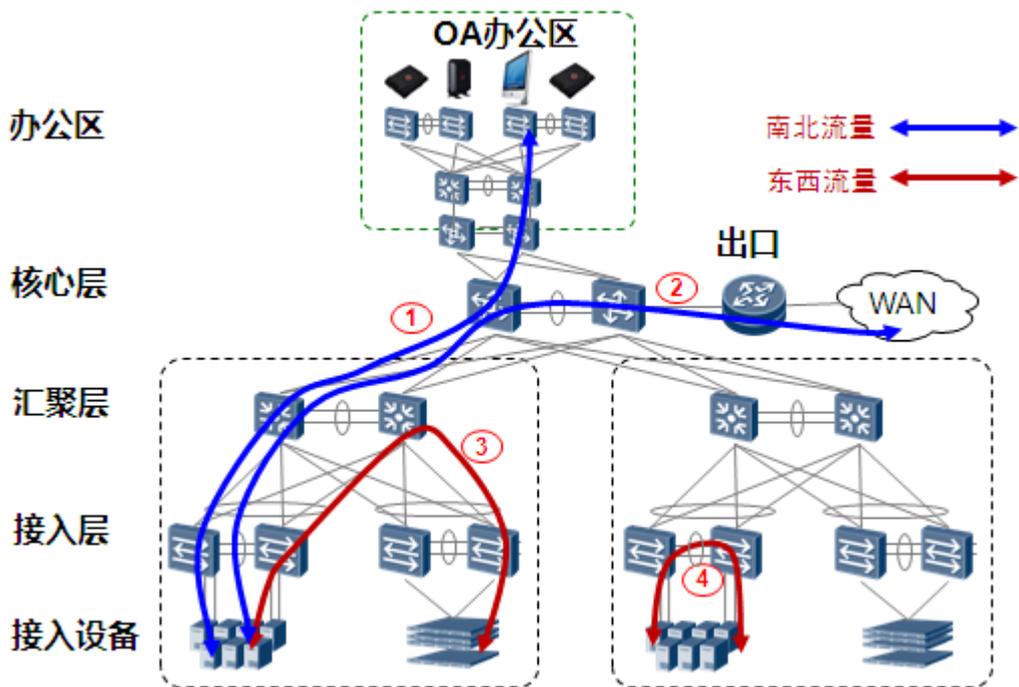
2.4.3 数据中心流量模型设计

流量分布类型

数据中心的内部流量分布可分为南北流量和东西流量两类。

- 南北流量：数据中心服务器与外部通信流量。包括键盘鼠标信息到虚拟机 VM 服务器流量、虚拟机 VM 屏幕显示 ICA 到终端流量、本地服务器访问远程数据中心的流量等
- 东西流量：数据中心内部服务器之间流量，包括云管理和业务服务器访问存储设备流量、服务器之间集群计算流量等。

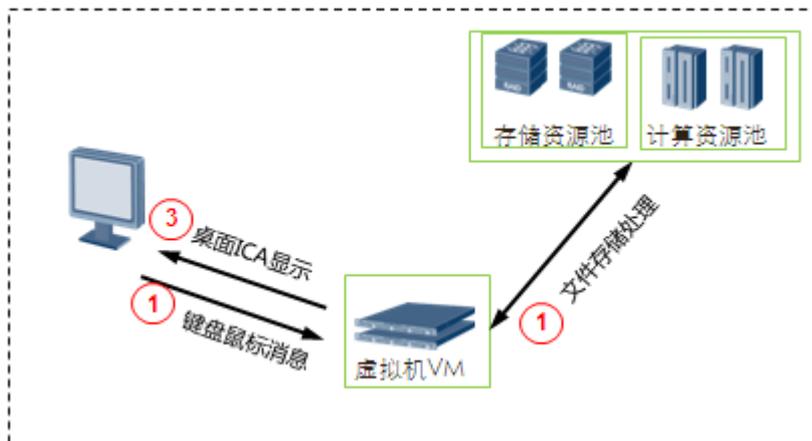
图2-10 数据中心内部流量分布类型



Office 文档应用流量模型

桌面云业务中，Office 文档应用的流量路径为：键盘鼠标消息 → 桌面虚拟机 → 文件存取处理 → 桌面虚拟机 → ICA 消息桌面显示。

图2-11 Office 文档应用流量模型

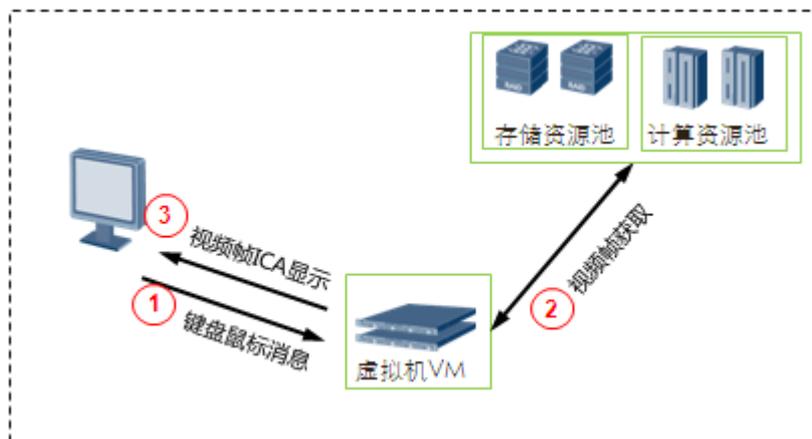


在 Office 文档应用中，虚拟机 VM 到终端网络质量影响云终端体验效果，存储获取慢影响文件打开速度，但不影响显示体验。

视频语音播放流量模型

桌面云业务中，视频语音播放的流量路径为：键盘鼠标消息 → 桌面虚拟机 → 从存储获取视频帧 → 桌面虚拟机 → 视频帧 ICA 显示。

图2-12 观看视频应用流量模型

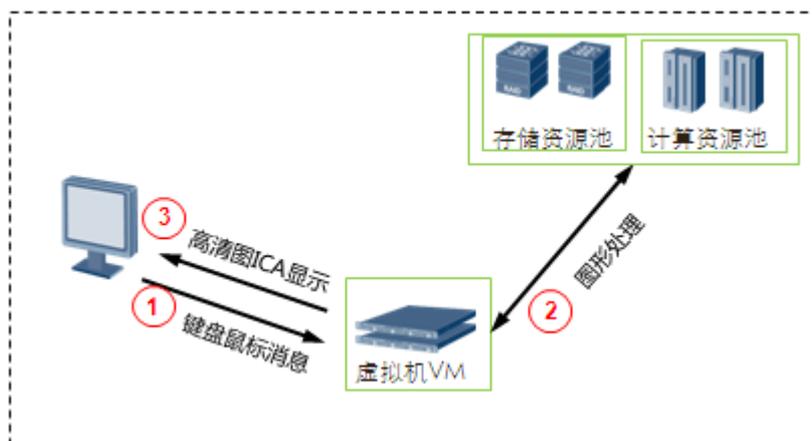


虚拟机 VM 到终端网络质量影响云终端体验效果，视频信息存储获取慢同样影响视频播放体验效果。

高清制图应用流量模型

桌面云业务中，高清制图应用的流量路径为：键盘鼠标消息 → 桌面虚拟机 → 图形计算处理 → 桌面虚拟机 → 高清图 ICA 显示。

图2-13 高清制图应用流量模型

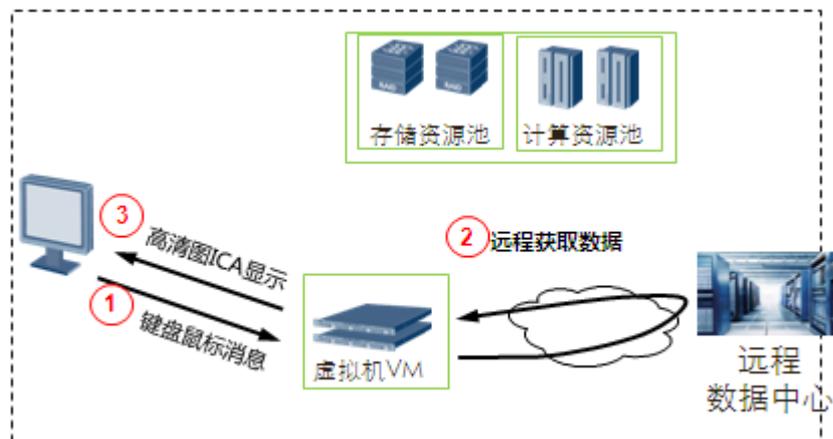


桌面虚拟机到终端网络质量影响显示体验效果，图形处理速度不影响显示，但高清图片差异变化导致 ICA 消息需要频繁刷新，带宽诉求高。

Portal 访问/Notes 应用流量模型：

桌面云业务中，Portal 访问/Notes 应用的流量路径为：键盘鼠标消息 → 桌面虚拟机 → 远程数据中心访问 → 桌面虚拟机 → ICA 桌面显示。

图2-14 Portal 访问/Notes 应用流量模型



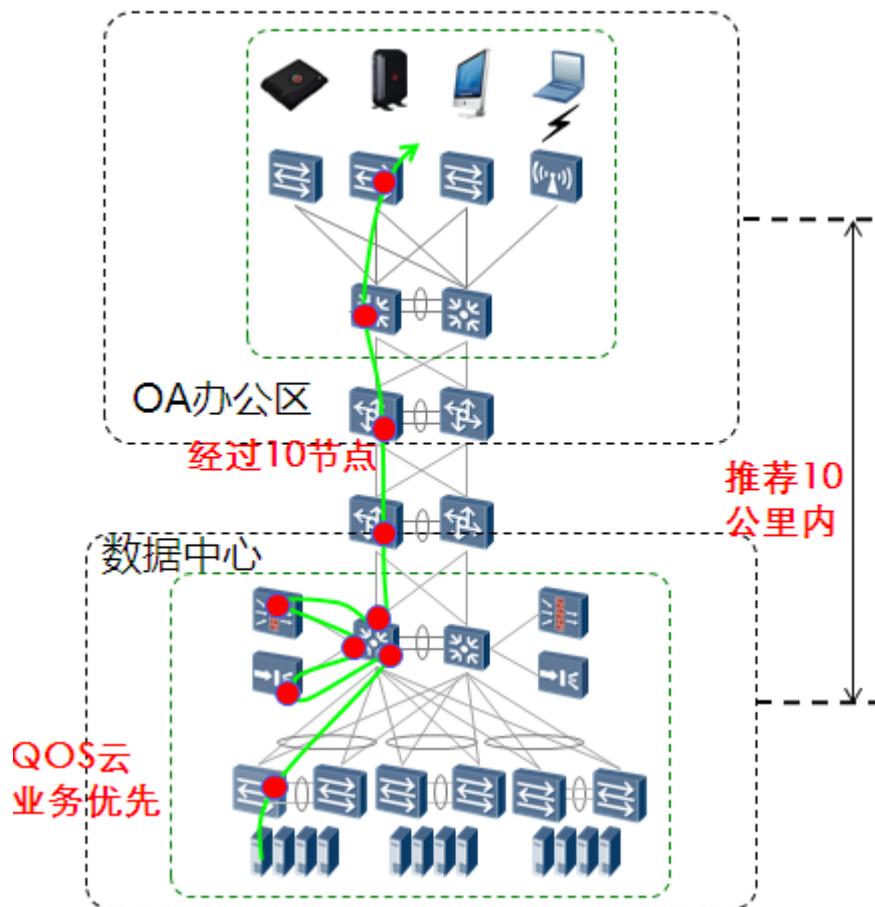
桌面虚拟机到终端网络质量影响云终端显示效果，远程获取数据慢并不影响显示体验效果（仅显示下载速度慢，但显示无卡顿）

2.5 网络质量设计

2.5.1 网络质量指标要求

对于 OA 集中办公桌面业务而言，承载网络质量的主要指标包括时延、丢包率和抖动，这几项指标的要求如图 2-15 所示。

图2-15 网络质量指标要求



时延要求

影响时延的因素主要是传输距离和经过设备节点数。因此在 OA 集中办公桌面云业务中，因按如下规则进行网络设计，以减少网络时延。

- 桌面云的所有办公区和数据中心之间距离不超过 10 公里内，原则不跨越城市。
- 云流量经过网络节点设备数最大不超过 15（包括防火墙和负载分担器）。
- QoS 部署保证云流量及时调度。

丢包率要求

影响丢包率的因素主要是网络拥塞。在 OA 集中办公桌面云业务中，部署万兆云园区带宽 20M 足够用，可避免拥塞。万一极端情况下发生拥塞，可部署 QoS 措施保证云流量不丢失。

抖动要求

影响抖动的主要因素是为经过设备节点数和拥堵调度不稳定造成。因此在 OA 集中办公桌面云业务中，因按如下规则进行网络设计，以降低网络抖动。

- 云流量经过网络节点设备数最大不超过 15（包括防火墙和负载分担器）。
- QoS 部署保证云流量均匀调度转发。

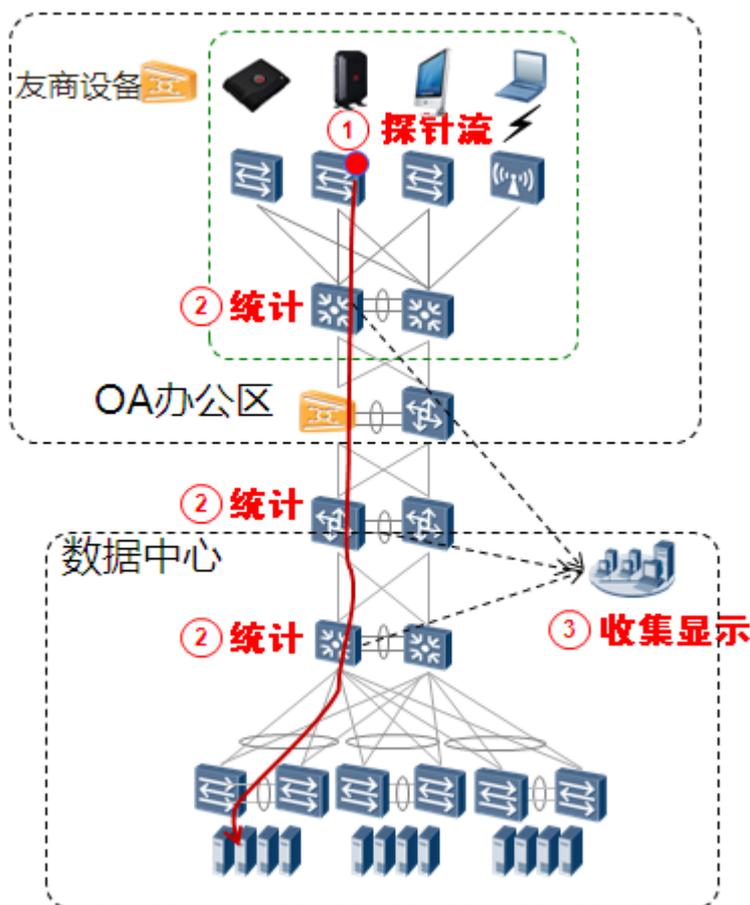
2.5.2 网络质量监控设计

OA 办公区云终端体验故障或待部署时，传统的承载网络的时延、丢包率等指标无法有效统计，因此也无法快速定位接入、汇聚、核心哪个层面可能存在质量问题。

通过基于 eSight 的网络质量监控方案，可以有效检测和统计各网段的质量指标，以便进行针对性的网络改造和优化。具体方案如下：

- 终端侧的接入交换机向云数据中心发送探针报文。
- 探针报文经过的各网络节点记录相应的网络质量数据。
- eSight 网管系统将各网络节点记录的网络质量数据进行收集，按规定算法计算出各项指标，并以图形化方式逐段予以显示。

图2-16 网络质量监控示意图



说明

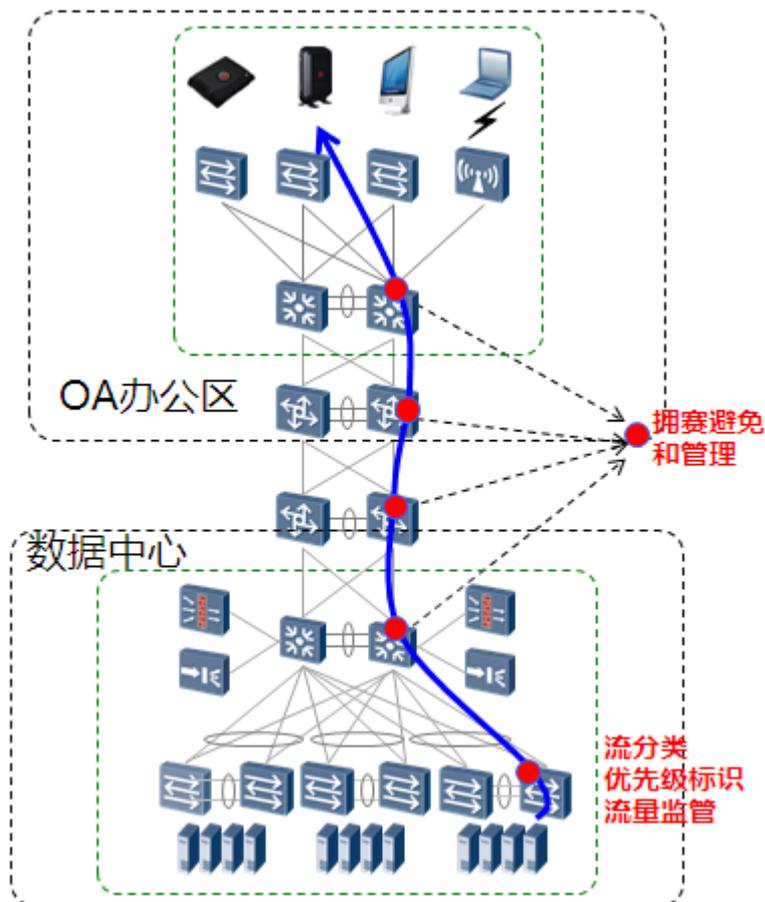
- 终端侧接入交换机需支持硬件探针，包括 S5700HI 及以上系列产品。
- 网管系统必须为华为公司 eSight 产品。
- 如果网络中间某些节点为非华为公司产品，则计算和显示时忽略掉相应网段，显示粒度变粗，但不影响整体方案。

2.5.3 QoS 设计

在 OA 集中办公桌面云方案中，要求承载网络优先保证 OA 云业务转发，避免网络拥塞造成的高时延、丢包率和抖动问题。具体的 QoS 部署的建议如下：

- 接入交换机通过协议类型和端口对业务进行流分类，并为业务流进行优先级重标记。优先级配置 802.1p 为 4、DSCP 为 34。
- 园区汇聚、核心交换机依据优先级标记，进行 QoS 拥塞避免和管理，优先保证云业务传输。
- 接入交换机可以通过 eSight 网管，通过 QoS 模板，批量进行云业务的 QoS 部署。
- eSight 网管可以全路径显示 DSCP 状态和更改，避免 QoS 部署失效。

图2-17 OA 集中办公桌面云 QoS 设计



2.6 可靠性设计

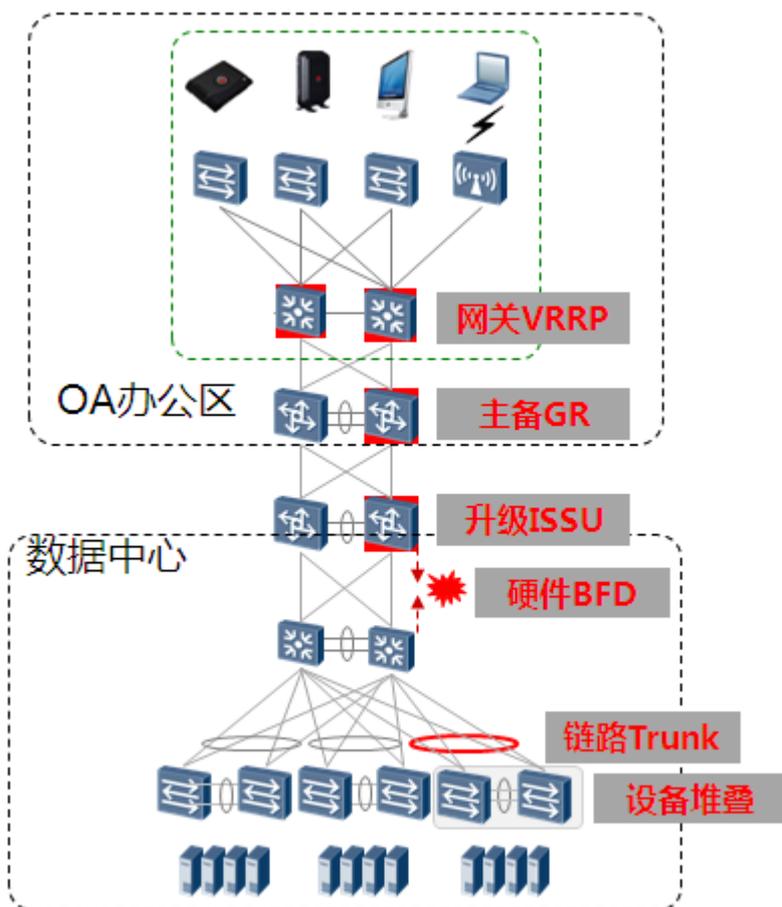
2.6.1 网络设备可靠性设计

网络设备的可靠性主要依靠冗余备份、快速故障检测和恢复两个方面来保证。到当网络某条链路、某节点设备发生故障时，在 10ms 内可以快速恢复，保证云用户的无缝体验。

具体的可靠性设计，可参考如下方案：

- 链路备份：采用 Eth-Trunk 链路双归上行。对于三层网络，可部署 IP FRR。
- 设备备份：双节点冗余，并部署 CSS/iStack 堆叠技术，对三层网络可部署 VRRP。
- 主控备份：配置双主控板，并部署 GR、NSR 协议。
- 升级可靠：部署 ISSU 升级不中断技术。
- 故障检测：部署硬件 BFD 和以太 OAM，实现 10ms 级的故障快速检测。

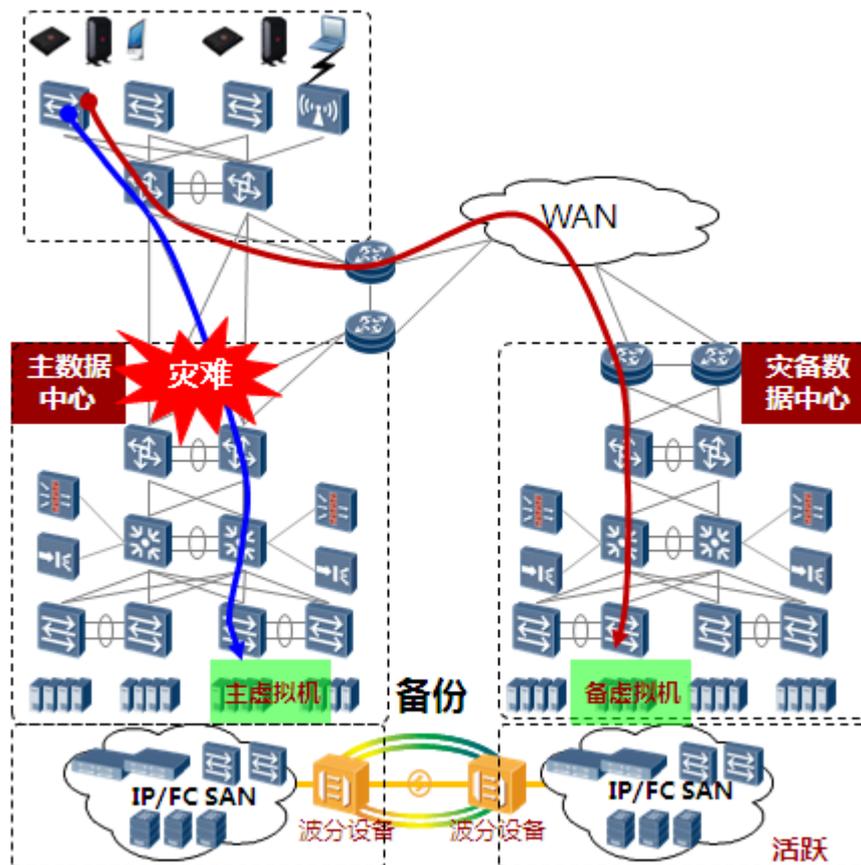
图2-18 网络设备可靠性设计



2.6.2 数据中心可靠性

数据中心可靠性主要是采用备份数据中心的方式，当主数据中心因自然灾害（例如大火、地震）等原因无法工作时，备份数据中心可以及时接管业务，保证业务不中断。

图2-19 数据中心可靠性部署



数据中心的灾备主要有冷热两种方式：

- 对于跨越 WAN 的灾备，主要采用夜间冷备份，RPO、RTO 目标为 24 小时。
- 对于同城灾备，一般采用光专线实时热备份，发生灾难时采用切换 DNS 方式实时将业务切换到备数据中心。RPO 目标为 20 分钟，RTO 目标为 2 小时。

📖 说明

- RPO：发生灾难前最后一次备份的时间点距离当前时间差。
- RTO：发生灾难后恢复物理系统环境的时间。

3 城域营业厅技术介绍

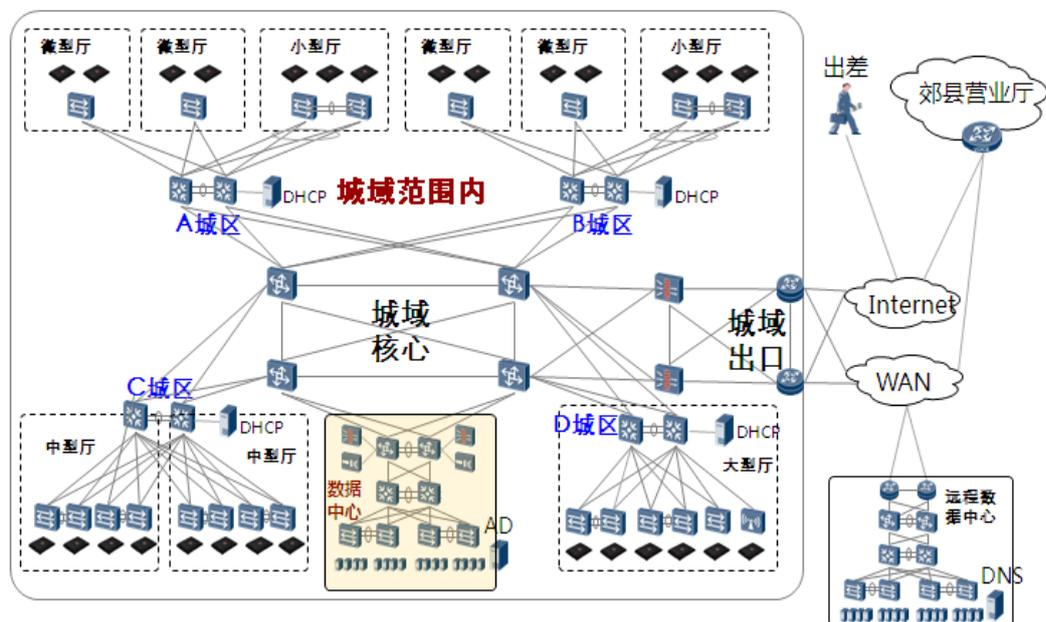
3.1 概述

企业在同一城市范围部署组网，以营业厅方式分散部署桌面云。适用于政府机关或者移动营业厅，例如城市公安系统、移动营业厅、呼叫中心等桌面云。

各个分散营业厅点通过城域以太技术和数据中心相连，完成桌面云业务应用。同城范围传输距离不长，时延较小能满足桌面云质量要求。

城域营业厅桌面云方案总体架构如图 3-1 所示。

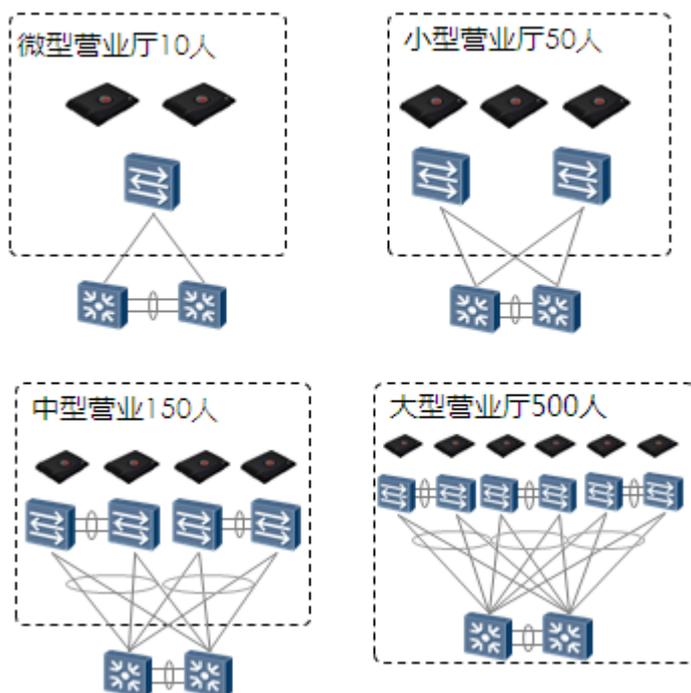
图3-1 城域营业厅桌面云总体架构



3.2 营业分厅组网设计

营业分厅的组网设计如图 3-2 所示。

图3-2 营业分厅组网设计



- 微型营业厅：10 人规模，一台二层交换机接入终端，连入城域汇聚交换机。
- 小型营业厅：50 人规模，两台二层交换机接入终端，双归连入城域汇聚交换机。
- 中型营业厅：150 人规模，两对二层交换机接入终端，双归连入城域汇聚交换机。
- 大型营业厅：500 人规模，N 对堆叠二层交换机接入终端，连入营业厅内部署的一对汇聚交换机，最终接入城域核心。

3.3 网络部署设计

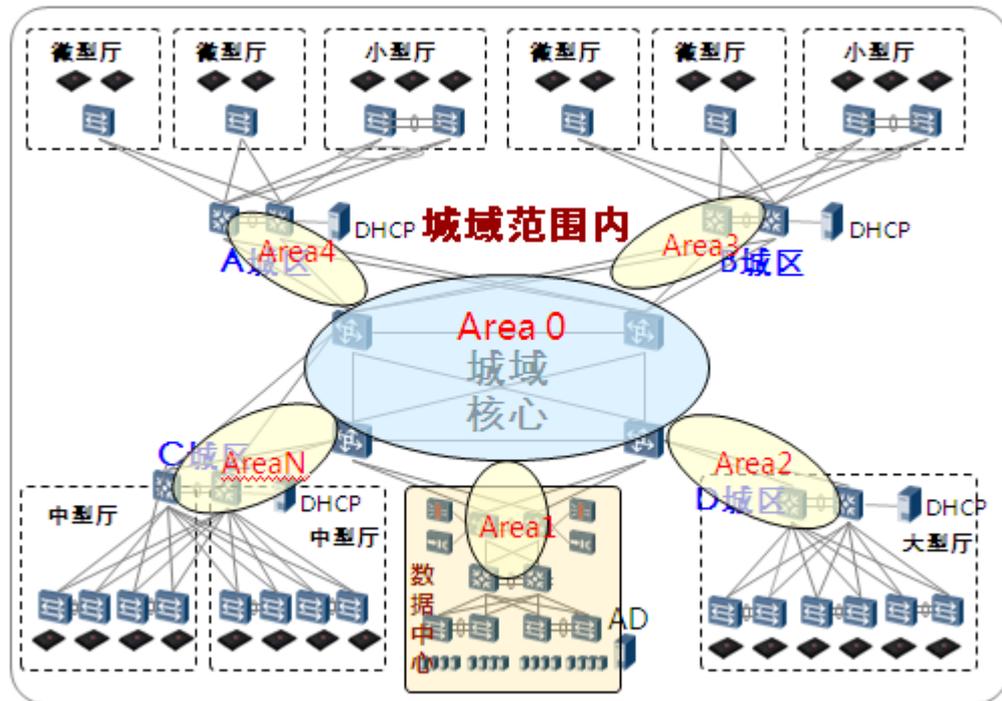
城域营业厅桌面云的网络部署方案主要有城域自建 OSPF 多区域、城域自建 OSPF 单区域和 MPLS L3VPN 三种方式。

3.3.1 城域自建 OSPF 多区域

在 OSPF 多区域部署方式中，城市核心层部署两台核心交换机，和各个分厅出口路由器以及数据中心核心交换机形成骨干 Area0（通过租用专线连接）。每个营业厅内部组网部署为不同的 OSPF 区域（Area 1、2……N），可配置 NSSA 或者 Stub 区域。

对于微、小营业厅来说，可以由出口路由器直接接入云终端，采用 OSPF 发布营业厅内部路由到外部 MPLS L3VPN 分厅。

图3-3 OSPF 多区域部署方式



本方案具体部署如下：

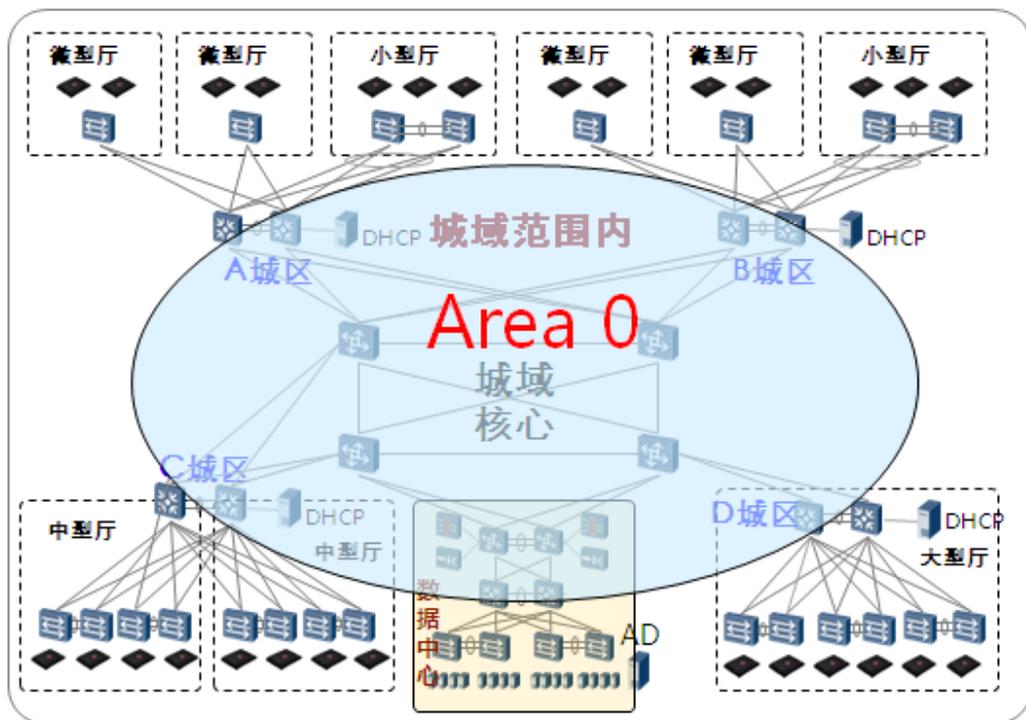
- 城市核心层部署四台核心交换机，和城域出口路由器以及数据中心核心交换机形成骨干 Area0（通过租用专线连接）。
- 每个城区汇聚交换机为不同的 OSPF 区域（Area ID 1,2,N），可配置 NSSA 或 STUB 区域。
- 营业厅内部采用二层交换机接入终端。

本方案中，区域以增量形式进行路由计算，每个城域汇聚层拓扑改变不会导致全网计算，SPF 计算规模大大降低。适合大中型城域中汇聚节点部署较多的情况。

3.3.2 城域自建 OSPF 单区域

城市核心层部署四台核心交换机，和城域出口路由器、所有城区汇聚层设备以及数据中心所有支持三层的设备形成骨干 Area0，不部署其他区域。

图3-4 OSPF 单区域部署方式

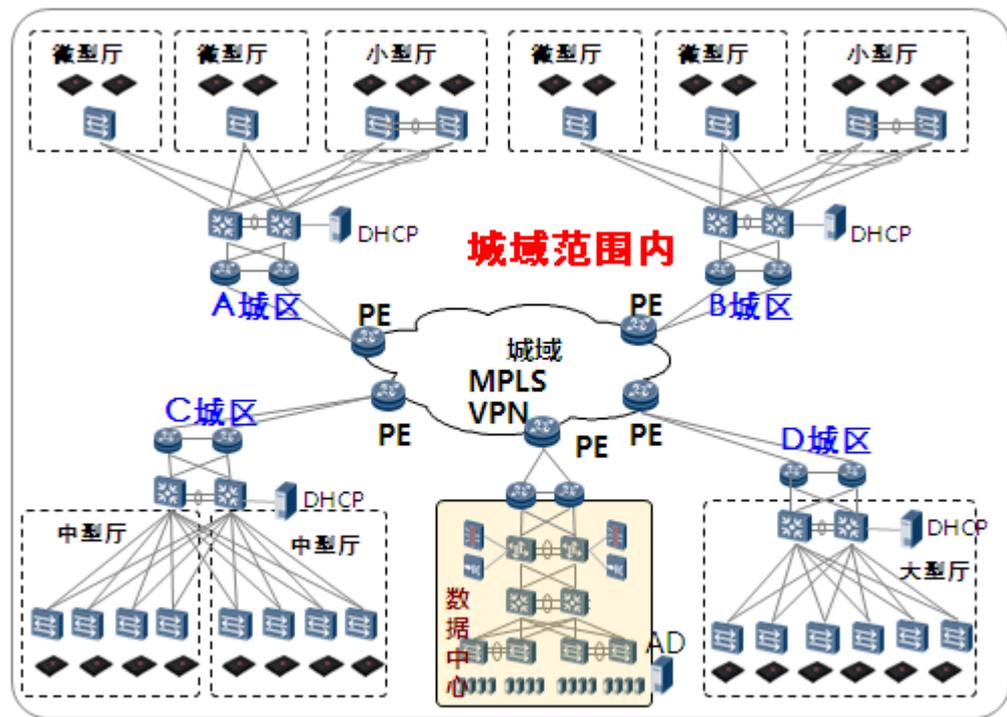


本方案的组网配置简单。但每个汇聚层拓扑改变都会触发全网 Totally 路由计算，OSPF SPF 计算规模也相对较大。适用于中小型城域、汇聚节点部署较少的情况。

3.3.3 租用 MPLS L3VPN

在 MPLS L3VPN 部署方式中，城域汇聚和数据中心通过城域 MPLS L3VPN 接入，NE40E 路由器作为出口 CE 和运营商 PE 相接，通过 MPLS 标签快速转发，实现桌面云应用。

图3-5 租用 MPLS L3VPN 部署方式



本方案可以通过 L3VPN 业务隔离访问，起到安全作用。流量经过多台 MPLS L3VPN 设备，时延抖动相对较大，对于高清图像处理桌面云业务体验效果一般。适合有业务访问隔离应用场景，例如如公安系统等。

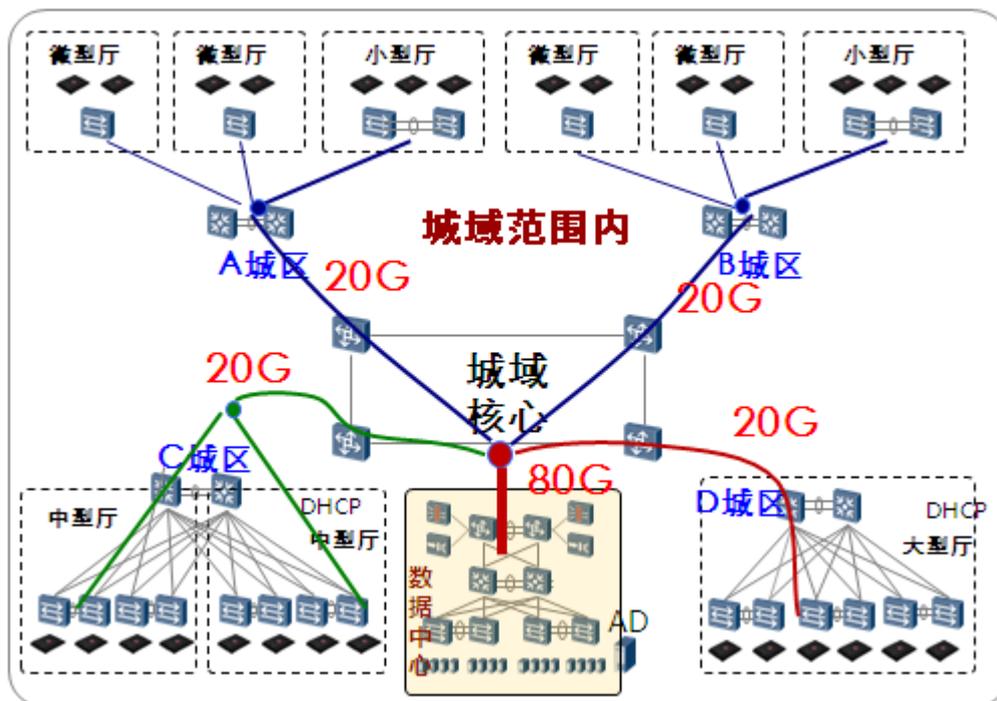
3.3.4 三种方式的对比

表3-1 城域营业厅桌面云网络部署方式对比

方式	组网概述	优点	缺点	适合场景
自建 OSPF 多区域	城域核心部署 Area 0，城域汇聚划分子区域	城域汇聚层拓扑改变增量计算，可限制计算规模	组网配置复杂，不能实现业务安全隔离	大中型城域营业厅
自建 OSPF 单区域	城域全网部署 Area 0 相连	组网配置简单	城域汇聚层拓扑改变触发全网路由重新计算	中小型城域营业厅
租用 MPLS L3VPN	城域汇聚通过 MPLS VPN 互联	通过 VPN 实现业务安全隔离	时延抖动相对较大，高清图像处理体验一般	适合有业务安全隔离应用场景，如公安系统等

3.4 带宽设计

图3-6 城域营业厅桌面云方案带宽设计



按照每个云用户 20M 带宽进行规划设计。

- A 城区：微型厅 50 个，每厅 10 人；小型厅 10 个，每厅 50 人。共需带宽 $50*10*20M+10*50*20M=20G$ 。
- B 城区：微型厅 50 个，每厅 10 人；小型厅 10 个，每厅 50 人。共需带宽 $50*10*20M+10*50*20M=20G$ 。
- C 城区：中型厅 2 个，每厅 500 人，共需带宽 $2*500*20M=20G$ 。
- D 城区：大型厅 1 个，每厅 1000 人，共需带宽 $1*1000*20M=20G$ 。

则桌面云数据中心需要的总带宽为 $20G + 20G + 20G + 20G = 80G$ 。

3.5 网络质量和监控设计

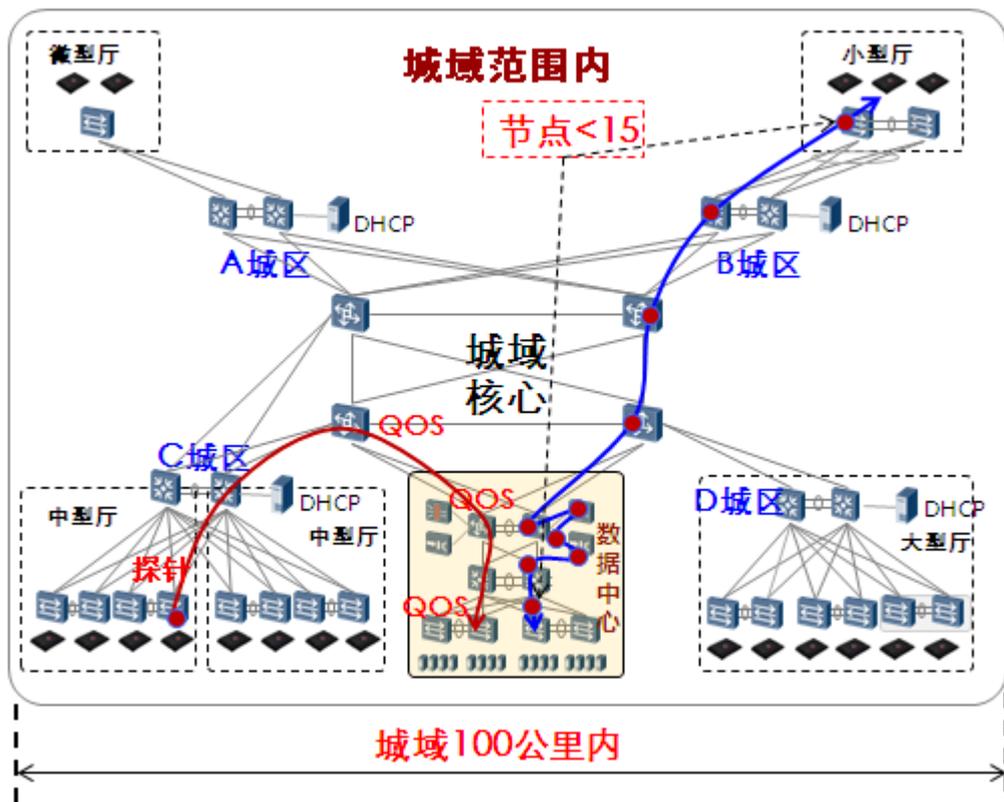
对于城域营业厅桌面云业务来说，为了保证时延、丢包率、抖动等网络质量，具体的网络设计要求如下：

- 城域距离小于 100 公里。
- 业务流经过设备节点数小于 15。
- 数据中心和城域核心需 QoS 部署保证云业务优先级。

另外，可以部署网络质量监控功能：

- 终端交换机发送探针流，从营业厅出口到城域汇聚、核心，最后到达数据中心。
- 路径网络设备进行数据统计。
- 网管收集统计并逐段显示时延、抖动质量。

图3-7 城域营业厅桌面云网络质量和监控设计



3.6 可靠性设计

城域营业厅桌面云业务的可靠性设计如图 3-8 所示。

图3-8 城域营业厅桌面云可靠性设计

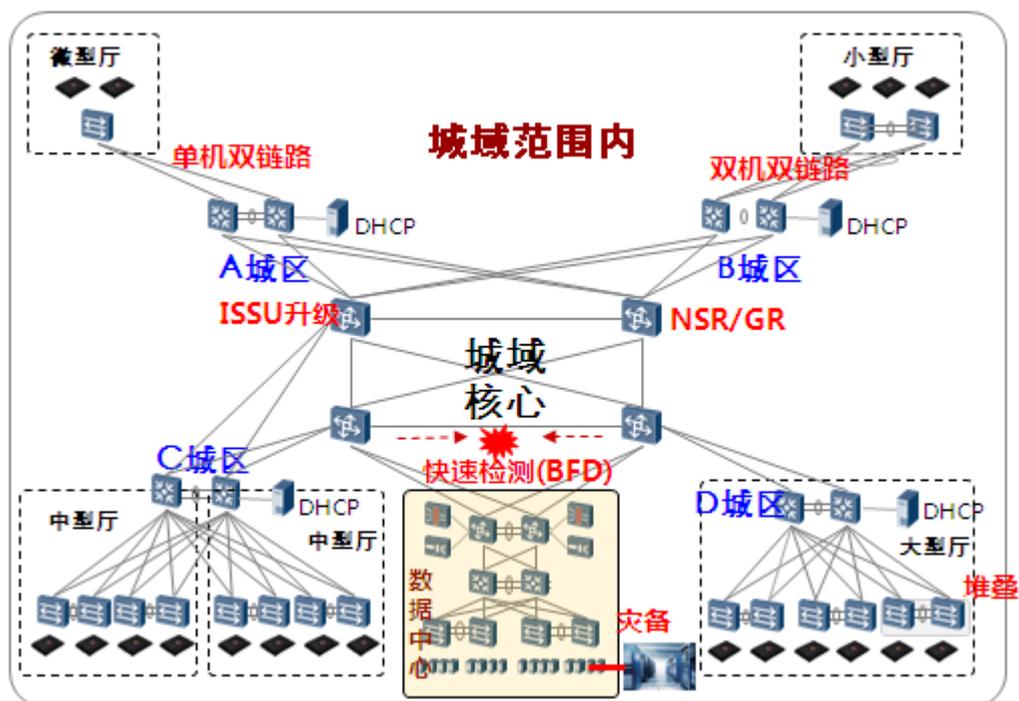


表3-2 各站点的可靠性措施

站点	可靠性措施
微型营业厅	双链路上行保证链路可靠性。
大中小型营业厅	采用双机冗余保证设备可靠性，双链路上行保证链路可靠性。
数据中心	根据业务安全系数，选择同城光纤或者异地 MPLS VPN 冷灾备。
骨干节点	单机部署 NSR、GR 以及硬件 BFD 故障检测、ISSU 无损升级等特性，可租用光纤链路负载分担。

3.7 产品选型

以下以 50 人规模的 100 个小型营业厅为例，说明设备的选型。

表3-3 城域营业厅桌面云方案产品选型

设备类型	部署位置	型号	单位	数量
服务器	数据中心	E6000 服务器 (2 路 6 核 CPU、72G 内存)	台	1800
核心交换机	数据中心	S9706	台	2

设备类型	部署位置	型号	单位	数量
接入交换机	数据中心	S5700	台	76
存储系统	数据中心	S3900（配置 132 块 600G SAS 硬盘）	套	50
核心交换机	城域网络	S9706	台	4
城域出口	城域网络	NE40	台	2
汇聚交换机	城域网络	S7706	台	6
接入交换机	营业分厅	S5700	台	200
云终端	营业分厅	TC G1945	台	5000

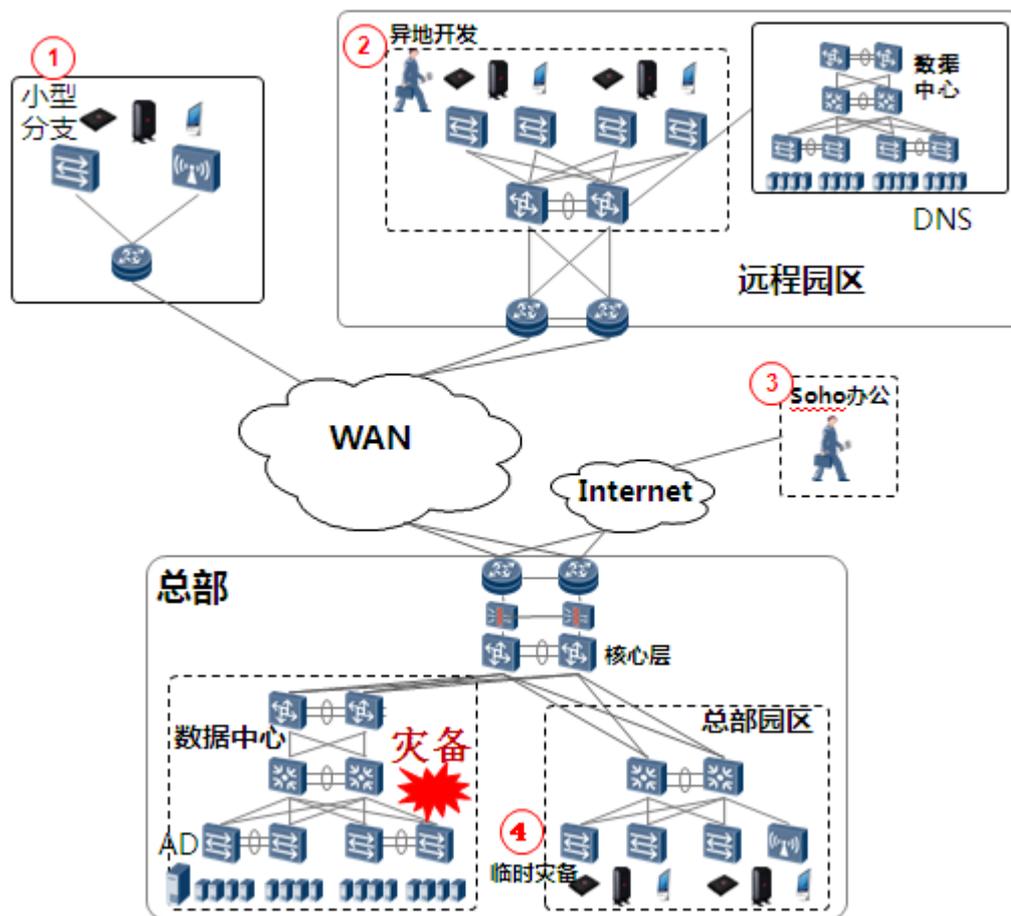
4 广域桌面云技术介绍

4.1 概述

4.1.1 典型组网

广域桌面云方案的典型组网如图 4-1 所示。主要包括小型分支接入、异地开发接入、SOHO 办公接入和临时灾备接入几种场景。

图4-1 广域桌面云方案典型组网



- 小型分支
一些小型分支，离数据中心距离不远，网络时延、抖动质量较好，通过跨广域 WAN 访问云服务器，实现 OA 等桌面云应用。
- 异地开发
总部员工出差分部需要接入桌面云，但出差员工不能直接访问分部园区数据中心（无用户存储），必须跨广域访问总部数据中心实现 OA 等桌面云应用。
- SOHO 办公
员工在家办公，通过家中接入 Internet 访问数据中心应用 OA 桌面云办公。
- 临时灾备
桌面云用户本地数据中心瘫痪，通过灾备方式，远程访问备份数据中心实现 OA 等桌面云应用。

4.1.2 广域应用业务和性能分析

广域桌面云业务应根据不同应用业务场景，灵活部署广域网，以满足桌面云时延和带宽方面的要求。

业务应用类型建议

- 小型分支：主用应用为桌面 OA 办公、少量研发应用和图形处理。
- 异地开发&灾备：主用应用为桌面 OA 办公、部分应用低清视频播放等。
- SOHO 办公：主要应用为桌面 OA 办公。

说明

桌面 OA 办公包含 Office 文档编辑（Word、Excel、PowerPoint 等）、工作流处理、邮件处理、文档下载常见应用。

带宽要求

- 小型分支：带宽价格适中，建议每用户 5M 带宽。
- 异地开发&灾备：专线资源宝贵，建议每用户 2M 带宽。
- SOHO 办公：带宽价格便宜，建议每用户 10M 带宽。

广域接入方式

- 小型分支：MPLS VPN 或 Internet SSL VPN。
- 异地开发&灾备：OTN 专线、MPLS VPN（少量）。
- SOHO 办公：通过 Internet，以 SSL VPN 方式接入。

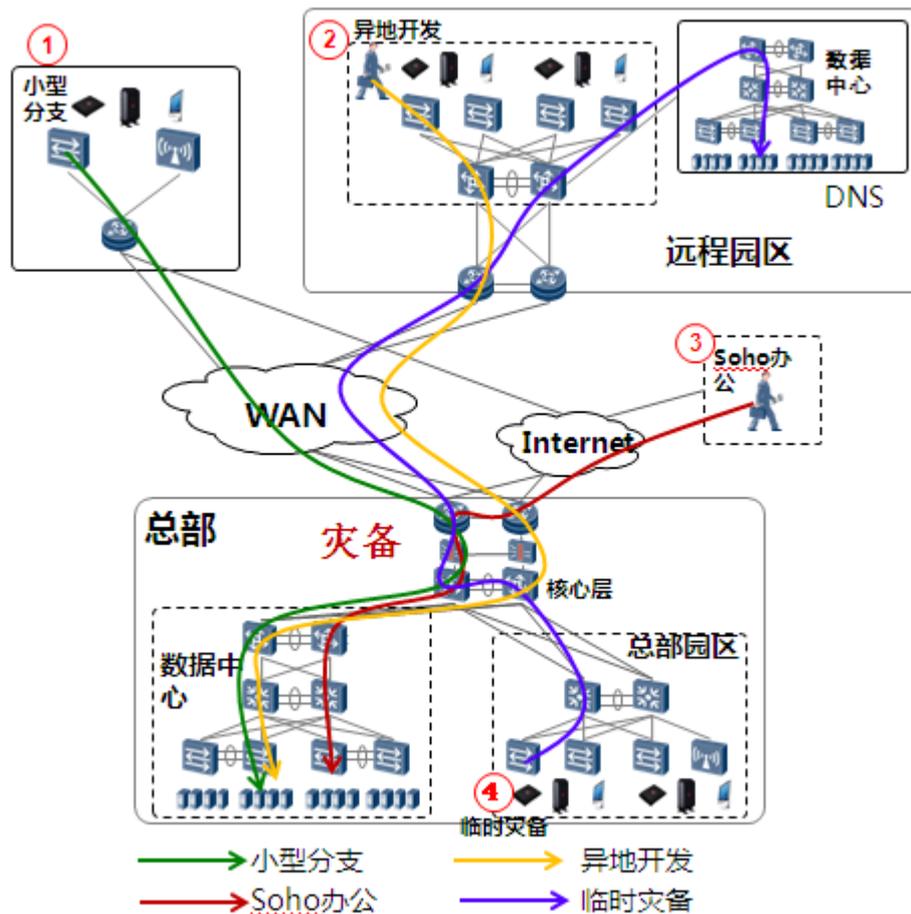
网络质量要求

- 小型分支：分支距离在 500km 以内，MPLS VPN 方式需保证经过路径节点少，延迟检测在 100ms 以内；Internet SSL VPN 方式需通过 SLA 保证时延。
- 异地开发&灾备：大型企业园区之间租用专线，2000km 范围内时延在 150ms 内。
- SOHO 办公：通过 Internet 的 SSL VPN 等多次中转，时延在 200ms 以上。

4.1.3 广域桌面云流量模型

广域桌面云业务的流量模型如图 4-2 所示。

图4-2 广域桌面云流量模型

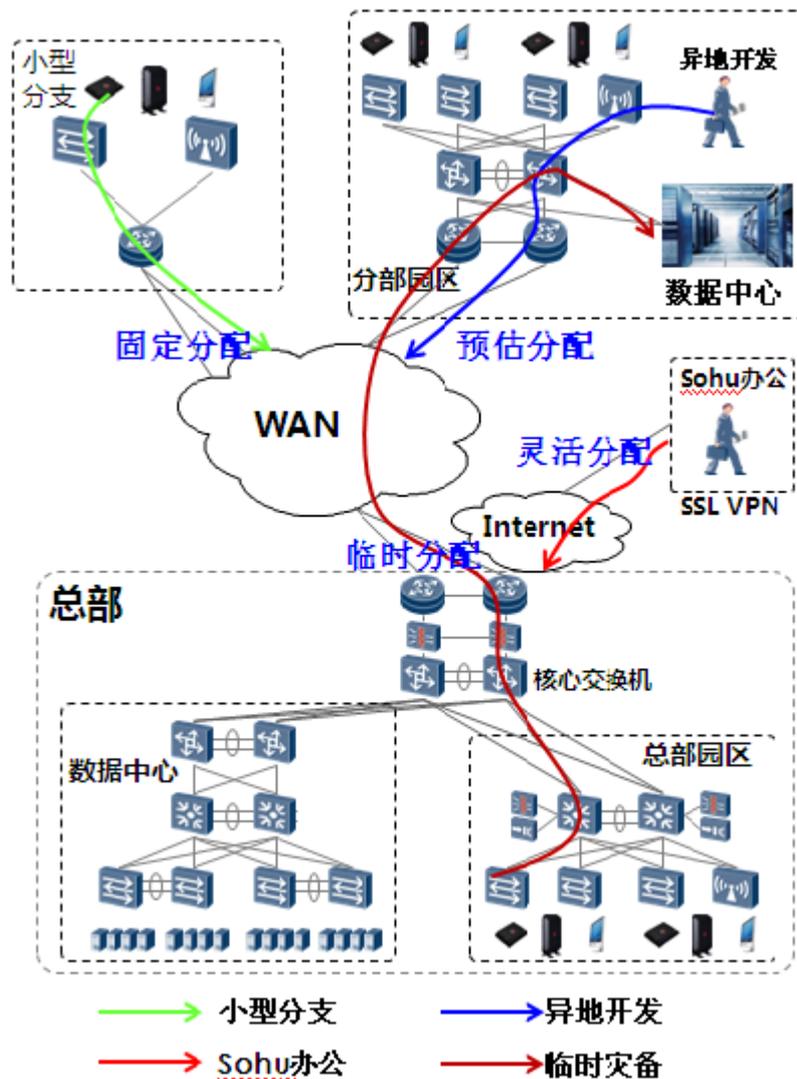


- 小型分支
分支用户云流量通过分支出口路由器出口，穿越 WAN 广域和 Internet 到达园区和数据中心。
- 异地出差
出差员工在异地园区接入，云流量通过园区出口路由器并跨越 WAN，到达园区和数据中心。
- SOHO 办公
在家办公员工通过 Internet 接入，云流量穿越 Internet 到达园区和数据中心。
- 临时灾备
用户云流量通过本地园区出口路由器出口，穿越 WAN 到达灾备数据中心。

4.2 带宽设计

针对不同的广域桌面云用户类型，采用不同的带宽分配方式。如图 4-3 所示。

图4-3 广域桌面云带宽分配



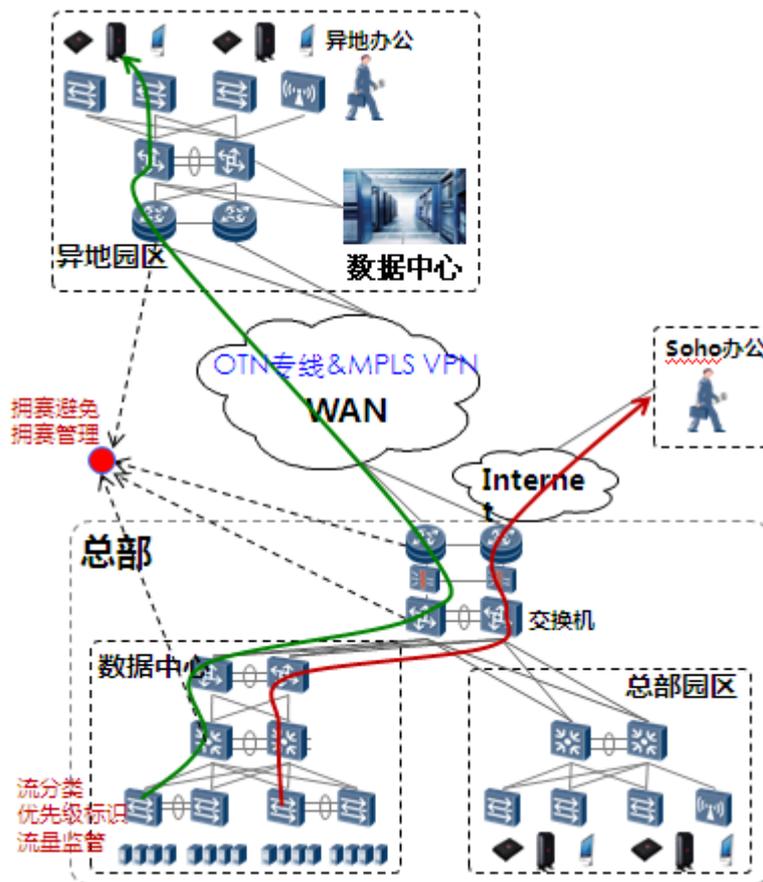
- 小型分支
分支桌面云用户人员固定，根据人数计算分配连入广域带宽。
- 异地办公
异地办公工作人员动态不定，根据统计值评估分配桌面云用户带宽预留。
- SOHO 办公
单用户接入，根据业务类型分配带宽，对于普通 OA 办公 2M 够用，图形应用较多用户需要 10M 甚至更高带宽。
- 临时灾备

桌面云用户灾备临时使用远程数据中心，会有大量用户批量占用带宽，考虑短暂临时性，每人分配 1M 带宽保证普通应用即可。

4.3 网络质量设计

广域桌面云的网络质量设计如图 4-4 所示。

图4-4 广域桌面云网络质量设计



异地园区或分支（穿越 WAN）

异地园区或分支的广域桌面云业务，一般需要部署 QoS，以保证桌面云业务的时延、丢包率和抖动等方面的质量要求。

- 终端和数据中心的接入层部署流分类、优先级标记和流量监管。
- 路径中间节点按优先级进行 QoS 调度，部署拥塞管理和拥塞避免。
- 如果桌面云业务中主要是 OA 办公应用，广域网可采用 MPLS L3VPN。
- 如果桌面云业务中有图形处理等低时延应用，则广域网需采用 OTN 专线。

另外，为了提高网络质量，还可以部署端到端的网络质量监控方案。通过 eSight 网管和网络设备的配合，检测、分析和显示各网段（不包括 WAN 部分）的时延、丢包率、抖动等质量数据，以便进行有针对性的网络改造和优化。

SOHO 办公（穿越 Internet）

员工在家办公，一般主要是 OA 办公业务，建议不支撑高质量业务。其网络质量设计主要包括如下内容：

- 数据中心的接入层部署流分类、优先级标记和流量监管。
- 数据中心/园区的中间节点按优先级进行 QoS 调度，部署拥塞管理和拥塞避免。
- 通过提升 Internet 接入带宽来提升 SOHO 接入的质量。

另外，为了提高网络质量，也可以部署网络质量监控方案。通过 eSight 网管和网络设备的配合，检测、分析和显示各网段（不包括用户家庭和 Internet 部分）的时延、丢包率、抖动等质量数据，以便进行有针对性的网络改造和优化。

4.4 广域加速设计

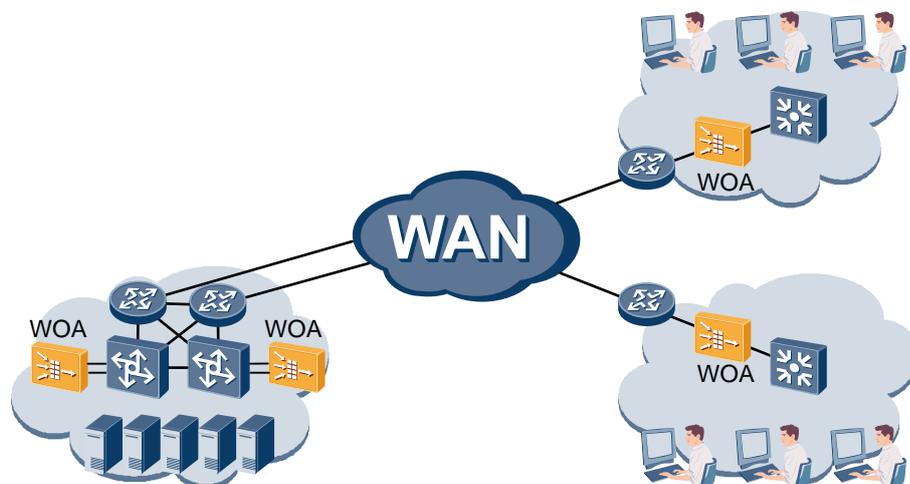
广域加速产生背景

在广域桌面云业务中，用户和数据中心之间是通过广域网络来实现互联的。而广域网通信的特点是带宽受限、时延较大、可靠性较低，这种情况将会导致用户在使用桌面云业务时出现响应缓慢、连接不稳定等情况，严重影响用户体验。

要解决上述问题，第一种方式是提升广域网本身的性能，例如增加带宽、优化网络拓扑、实时合理的 QoS 调度等等。但这种方法对于大部分企业来说并不适用，因为很多企业并无自己的广域网，而是租用运营商的网络，无法实施对于广域网的优化。

另一种较为实际的方案，就是在通信两端（例如分支机构和数据中心之间）部署广域网应用加速系统，通过 WOA（广域网优化加速技术）来提升业务体验。如图 4-5 所示。

图4-5 广域加速部署



广域加速的主要技术

广域网的主要问题一是带宽不足，二是网络时延较大。而造成网络时延大的主要原因又包括两方面：传输协议效率低下（例如 TCP 协议的多次握手机制、滑动窗口过小等等）、应用层协议效率低下（例如反复请求、交互/等待机制、数据包碎小等等）。

以远程打开 5MB 的 Word 文档的过程为例，大约要进行 700 次的操作请求（550 次读请求、150 次其他请求），以 WAN 通信的单次响应时间为 250ms 计算，则应用的响应操作时间将超过 175 秒，这是用户不可承受的事情。

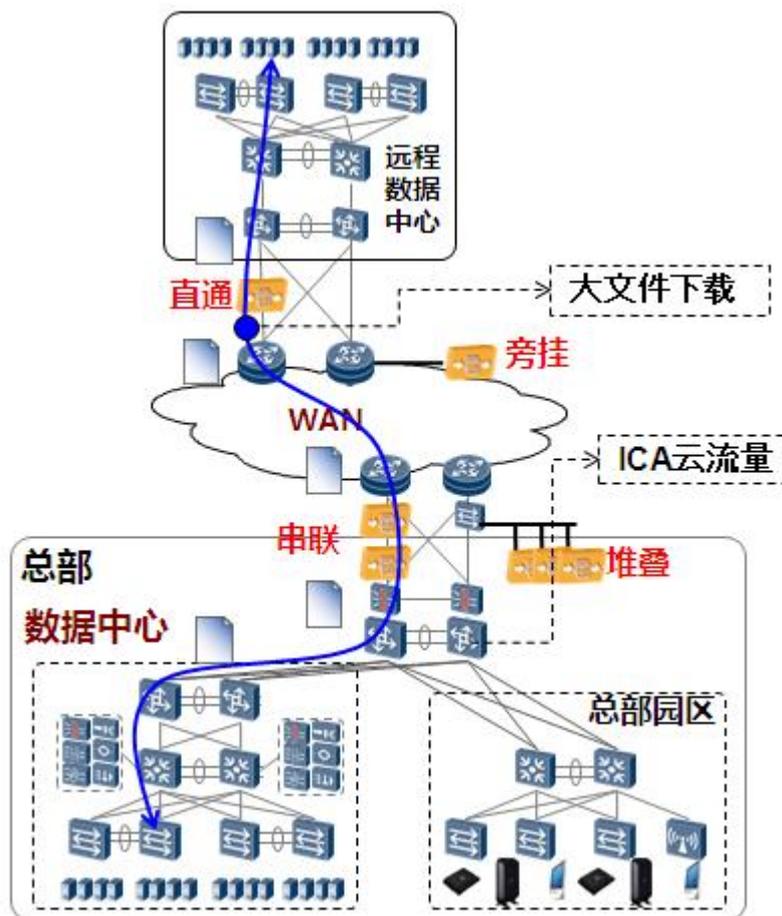
广域网应用加速主要从如下三方面来优化传输性能，提升用户体验：

- 数据优化：通过数据压缩、数据缓存、避免重传数据等技术来节省带宽。
- 传输优化：通过改进 TCP 慢启动机制、改进拥塞管理机制、改进确认/重传机制、改进滑动窗口机制、TCP 复用、SSL 优化等技术，加快网络传输速度。
- 应用优化：通过改进常用应用协议（例如 CIFS、MAPI、NFS、HTTP、HTTPS、FTP 等）的交互应答机制，来提升应用协议效率，加快应用处理速度。例如本地代理、本地应答、数据缓冲、预取/先读/后写等等。

广域加速的组网形式

广域加速的组网形式主要有直通、旁挂、串联和堆叠几种，如图 4-6 所示。

图4-6 广域加速的组网形式



- 直通方式：部署简单，无备份和并行功能。
- 旁挂方式：过滤流量加速，无并行功能。
- 串联方式：不同加速器执行不同加速角色。
- 堆叠方式：具备大规模并行加速和互备份功能。

4.5 性能路由设计

性能路由可以针对指定具体流量，实时监控时延、丢包或者抖动等网络质量，如果不符合业务要求，则智能切换 ISP 出口，寻找满足质量要求的出口。

在广域桌面云方案中，桌面云用户部署在分支，和总部数据中心跨广域交互云业务数据，租用两个 ISP 的不同链路，云数据优先选择 ISP1 的链路跨越 WAN，但是 ISP1 的链路经常发生拥堵，造成云业务时延较长体验差。

此时园区出口的 AR 路由器可通过性能路由，监控用户桌面云业务网络质量状态，时延超过容忍值时智能选择满足要求出口转发云业务流量。

图4-7 性能路由设计

