

YD

中华人民共和国通信行业标准

YD 5193—2014

互联网数据中心(IDC)工程设计规范

Design Specifications for
Internet Data Center Engineering

2014-05-06 发布

2014-07-01 实施

中华人民共和国工业和信息化部 发布

中华人民共和国通信行业标准

互联网数据中心(IDC)工程设计规范

Design Specifications for Internet Data Center Engineering

YD 5193—2014

主管部门：工业和信息化部通信发展司

批准部门：中华人民共和国工业和信息化部

施行日期：2014 年 7 月 1 日

北京邮电大学出版社

2014 北京

中华人民共和国工业和信息化部

公 告

2014 年 第 32 号

工业和信息化部批准《不干胶标签印刷机》等 1208 项行业标准(标准编号、名称、主要内容及起始实施日期见附件 1),其中机械行业标准 471 项,汽车行业标准 32 项,船舶行业标准 70 项,航空行业标准 111 项,化工行业标准 137 项,冶金行业标准 69 项,建材行业标准 30 项,石化行业标准 14 项,有色金属行业标准 6 项,轻工行业标准 89 项,纺织行业标准 49 项,兵工民品行业标准 79 项,核行业标准 15 项,电子行业标准 2 项,通信行业标准 34 项。批准《锰硅合金(FeMn68Si16)》等 39 项冶金行业标准样品(标准样品目录及成分含量见附件 2)。

以上机械行业标准由机械工业出版社出版,汽车行业标准及化工、有色金属工程建设行业标准由中国计划出版社出版,船舶行业标准由中国船舶工业综合技术经济研究院组织出版,航空行业标准由中国航空综合技术研究所组织出版,化工行业标准由化工出版社出版,冶金行业标准由冶金工业出版社出版,建材行业标准由建材工业出版社出版,石化行业标准由中国石化出版社出版,轻

工行业标准由中国轻工业出版社出版,纺织行业标准由中国标准出版社出版,兵工民品行业标准由中国兵器工业标准化研究所组织出版,核行业标准由核工业标准化研究所组织出版,电子行业标准由工业和信息化部电子工业标准化研究院组织出版,通信行业标准由人民邮电出版社出版、通信工程建设行业标准由北京邮电大学出版社出版。

附件: 1. 1208 项行业标准编号、名称、主要内容等一览表(略)

2. 39 项冶金行业标准样品目录及成分含量(略)

工业和信息化部

2014 年 5 月 6 日

前 言

本规范根据工业和信息化部“关于安排 2009 年《通信工程建设标准》编制计划的通知”(工信部通函[2009] 98 号)的要求编制。

本规范主要规定了互联网数据中心(IDC)的业务、系统组成、IDC 分级、机房设施子系统、网络子系统、资源子系统、业务子系统、管理子系统、网络与信息安全、计费、IP 地址与码号、服务质量、能耗、设备配置等。

本规范中用黑体字标注的 1.0.3 条、1.0.4 条为强制性条文，必须严格执行。

本规范由工业和信息化部通信发展司负责解释、监督执行。规范在使用过程中，如有需要补充或修改的内容，请与部通信发展司联系，并将补充或修改意见寄部通信发展司(地址：北京市西长安街 13 号，邮编 100804)。

主编单位：中国移动通信集团设计院有限公司

主要起草人：崔海东 雷 鸣

参编单位：江苏省邮电规划设计院有限责任公司

主要参加人：卢智军 陈月琴

目 次

1	总则	1
2	术语和符号	2
3	业务	4
4	系统组成	5
5	IDC 分级	6
6	机房设施子系统	7
6.1	机房要求	7
6.2	机架要求	9
6.3	电气、空调、布线与安防	11
7	网络子系统	14
7.1	网络结构	14
7.2	路由	16
8	资源子系统	17
9	业务子系统	18
10	管理子系统	19
10.1	系统设置	19
10.2	网络管理	19
10.3	资源管理	21
10.4	业务管理	22
10.5	运营管理	22
11	网络与信息安全	24
11.1	安全目标	24
11.2	安全技术措施	24
11.3	安全管理	25

11.4 备案管理与有害信息监测	25
12 计费	26
13 IP 地址与码号	27
13.1 IP 地址	27
13.2 码号	27
14 服务质量	28
15 能耗	29
16 设备配置	30
附录 A 本规范用词说明	31
引用标准名录	32
条文说明	33

1 总 则

1.0.1 本规范适用于互联网数据中心(IDC)新建工程设计,改扩建工程设计在合理利用原有设施的基础上参照本规范执行。

1.0.2 IDC的设计应遵循开放性的原则,设计的系统应具有标准化、模块化、可靠性、可扩充性。

1.0.3 工程中所采用的电信设备,必须取得工业和信息化部“电信设备进网许可证”。

1.0.4 在我国抗震设防烈度7烈度以上(含7烈度)的地区公用电信网中使用的主要电信设备必须经电信设备抗震性能检测合格。

1.0.5 本规范与国家有关标准、规范相矛盾时,应按国家标准、规范的相关规定办理。

1.0.6 在特殊条件下,执行本规范中的个别条款有困难时,应充分论述理由,提出采取措施的报告并呈主管部门审批。

2 术语和符号

英文缩写	英文名称	中文名称
ASP	Application Service Provider	应用服务提供商
BGP	Border Gateway Protocol	边界网关协议
BSS	Business Support System	业务支撑系统
CDN	Content Distributed Network	内容分发网络
DDoS	Distributed Deny of Service	分布式拒绝服务攻击
IaaS	Infrastructure as a Service	基础设施即服务
ICP	Internet Content Provider	互联网内容提供商
IDC	Internet Data Center	互联网数据中心
IDS	Intrusion Detection System	入侵检测系统
IP	Internet Protocol	互联网协议
IPS	Intrusion Prevention System	入侵预防系统
ISIS	Intermediate System To	中间系统到中间系统
	Intermediate System	
ISP	Internet Service Provider	互联网服务提供商
KVM	Keyboard Video Mouse	多计算机切换器
MAC	Media Access Control	介质访问控制
NAS	Network Attached Storage	网络连接存储
OSPF	Open Shortest Path First	开放式最短路径优先
OSS	Operation Support System	运营支撑系统
PaaS	Platform as a Service	平台即服务
PUE	Power Usage Effectiveness	能源利用效率
QoS	Quality of Service	服务质量

RAID	Redundant Array of Independent Disk	独立冗余磁盘阵列
SaaS	Software as a Service	软件即服务
SAN	Storage Area Network	存储区域网络
SNMP	Simple Network Management Protocol	简单网络管理协议
SSL	Secure Sockets Layer	套接字安全层
UPS	Uninterrupted Power Supply	不间断电源
VIP	Very Important Person	重要用户
VLAN	Virtual Local Area Network	虚拟局域网
VPN	Virtual Private Network	虚拟专用网

3 业 务

3.0.1 IDC 应提供基本业务,包括以下种类:

1. VIP 机房出租;
2. 主机托管;
3. 机架出租;
4. 服务器出租;
5. 虚拟机出租;
6. 带宽出租;
7. IP 地址出租。

IDC 可根据电信业务经营者的要求提供更多种类的基本业务。

3.0.2 IDC 可提供增值业务,作为在基本业务之外用户选购的附加服务,主要包括:

1. 安全防护类,包括防火墙出租、VPN 接入、病毒防范、入侵检测、防 DDoS 攻击、流量清洗、网页防篡改、安全扫描、安全评估等;
2. 数据存储类,包括在线存储、在线备份、数据备份及异地备份等;
3. 流量管理类,包括负载均衡、SSL 加速、流量统计分析等;
4. 维护管理类,包括远程维护、设备代理监测、设备代理维护等;
5. 内容管理类,包括网站镜像、网页加速、应用加速、CDN 等;
6. 系统集成类,包括设备安装和升级、网站设计与建设等;
7. 云计算概念类,包括 IaaS 类业务、PaaS 类业务、SaaS 类业务等。

IDC 可根据电信业务经营者的要求提供更多种类的增值业务。

4 系统组成

4.0.1 IDC 应包含机房设施子系统、网络子系统、资源子系统、业务子系统、管理子系统五大逻辑功能部分。

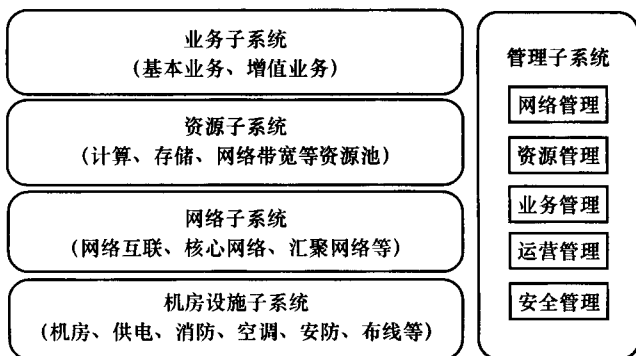


图 4.0.1 IDC 系统组成图

1. 机房设施子系统为 IDC 提供机房、供电、消防、空调、安防、布线等系统。
2. 网络子系统为资源子系统和业务子系统提供网络环境。
3. 资源子系统为业务子系统提供开展业务运营所需的基础资源池,包括计算资源、存储资源、网络资源、软件应用能力资源等。
4. 业务子系统提供 IDC 的基本业务和增值业务。
5. 管理子系统为 IDC 的运营维护提供必要的管理支撑,包括网络管理、资源管理、业务管理、运营管理、安全管理等。

5 IDC 分级

5.0.1 IDC 应根据运营需要分为不同级别,可划分为 A、B、C 三级,不同级别对外可在可靠性、绿色节能、安全性、服务质量和水平等方面予以区别,对内可在各子系统技术要求方面有所区别。

5.0.2 IDC 内所装业务系统的运行中断将造成重大损失的,IDC 应为 A 级;IDC 内所装业务系统的运行中断将造成较大损失的,IDC 应为 B 级;不属于 A 级或 B 级的 IDC 应为 C 级。设计时应根据 IDC 的业务需求确定所属级别。

5.0.3 一个 IDC 内的不同部分可根据业务需求按不同的标准进行设计。

6 机房设施子系统

6.1 机房要求

6.1.1 IDC 机房应符合 GB 50174《电子信息系统机房设计规范》和 YD 5003《通信建筑工程设计规范》的各项规定,机房环境要求可参照 YD/T 1821《通信中心机房环境条件要求》的相关规定。

6.1.2 IDC 机房应设置在电力供应充足、交通通讯方便、配套设施齐全、安全可靠、自然环境清洁的地点,宜选择基础设施条件较好的城市开发新区、城郊或城市边缘地带。

6.1.3 IDC 机房功能分区应包括:主机房区、支持机房区和辅助房间区。

1. 主机房区是 IDC 生产运行的核心机房区域,可包括网络子系统机房(区)、资源子系统机房(区)、管理子系统机房(区)、出租/托管业务机房(区)等。出租/托管业务机房(区)可根据电信业务经营者的业务需求进一步分割,分为一般用户区、VIP 用户区等。主机房区中的不同功能区域可以是一个独立的机房也可以是隔离下的独立分区。

2. 支持机房区包括变配电室、柴油发电机房、电力电池室、空调机房、消防设施用房、消防和安防控制室等。

3. 辅助房间区可包括客户维护操作室(区)、客户接待室(区)、客户休息室(区)、业务参观及展示区域、门厅、值班室、更衣间等。A 级和 B 级 IDC 宜在设置齐全的辅助房间,C 级可根据电信业务经营者的业务需求灵活设置。

6.1.4 IDC 机房面积应根据电信业务经营者的业务发展规划合

理确定,宜根据集中化原则建设大容量 IDC。辅助房间区使用面积占主机房区,使用面积的比例宜符合表 6.1.4 的规定。

表 6.1.4 机房面积建议

IDC 级别	A	B	C
辅助房间区使用面积(占主机房区使用面积的比例下限)	10%~15%	10%~15%	8%~10%

6.1.5 IDC 机房建筑的耐久年限和耐火等级应符合表 6.1.5 的规定。

表 6.1.5 机房耐久年限和耐火等级建议

IDC 级别	A	B	C
耐久年限	50 年以上	50 年以上	50 年
耐火等级	不低于二级	不低于二级	不低于二级

6.1.6 IDC 机房主要部分的楼面均布活荷载要求,可按表 6.1.6 的要求,其他机房应根据相关的规范规定。

表 6.1.6 楼面均布活荷载要求

IDC 级别	A	B	C
主机房区(kN/m ²)	10~12	8~10	6~8
电力电池室(kN/m ²)	16 (电池组四层双列摆放)	16 (电池组四层双列摆放)	10

IDC 主机房区的楼板吊挂荷载可为 1.2 kN/m²。

改造的 IDC 机房应根据荷载要求采取加固措施,并应符合现行的 GB 50367《混凝土结构加固设计规范》的规定。

6.1.7 IDC 主机房区梁下净高由气体灭火管道高度、工艺生产要求的净高、活动地板高度或送风风管高度组成,尺寸要求见表 6.1.7。

表 6.1.7 主机房区梁下净高要求

气体灭火管道高度	工艺生产要求的净高	活动地板高度 (下送风时)	送风风管高度 (上送风时)
200 mm	2 500~3 000 mm	400~1 200 mm	250~700 mm

6.1.8 IDC 主机房区设置在二楼或二楼以上时,应有载货电梯到达主机房区所在楼层,货运电梯核定载重量不应小于 2 000 kg,电梯轿厢尺寸不宜小于 1 500 mm(宽)×2 600 mm(深),A 级和 B 级 IDC 同时应设置载客电梯。

6.1.9 IDC 主机房区内部各类通信设备的布局,在预留发展空间的前提下应相对集中。主机房一般应采用矩形以提高面积的有效利用率。主机房区内一般不做隔断,有分隔需求时应使用通透式钢笼隔断,便于空调气流循环,通透式钢笼隔断设置不应影响机房的消防疏散。

6.1.10 IDC 主机房区应设置气体灭火系统和火灾自动报警系统,消防设计应符合国家、行业有关标准和规范。其他区域的消防设计应符合国家及行业的有关标准及规范。

6.2 机架要求

6.2.1 IDC 主机房内的设备机架(包括 IDC 自有系统用机架、出租用机架)的外形尺寸宜采用:2 200 mm×600mm×1 000 mm(高度×宽度×深度)。在需要时,其尺寸变动范围宜为:高度在 2 000 ~ 2 200 mm 之间;宽度在 600~900 mm 之间;深度在 900~1 200 mm 之间。

6.2.2 IDC 主机房内支持的设备机架平均运行功率宜符合表 6.2.2 的要求。

表 6.2.2 单机架平均运行功率

主机房区域	高功率区	中功率区	低功率区
单机架平均运行功率 (kW/架)	>6 kW/架	>3 kW/架且 ≤ 6 kW/架	≤ 3 kW/架

注:IDC 机房可按机架运行功率不同分区布置,同一 IDC 机房模块宜设计选用相同机架,平均运行功率。机架应按设计运行功率加载设备。

6.2.3 A 级和 B 级 IDC 主机房内每个机架的架内宜配置两路负载分担或主备工作方式的电源分配模块。

6.2.4 机架内不宜设置普通电源插座,设备不应跨机架取电。

6.2.5 机架上宜根据需求设置能耗统计仪表,实时监测本机架耗电情况。

6.2.6 机架应设有接地点,并配置供设备接地用的接地汇流排。

6.2.7 A 级和 B 级 IDC 主机房气流组织应形成冷通道和热通道,机架排列布置应采用“面对面、背对背”的排列方式,相邻两列设备的吸风面(正面)安装在冷通道上,排风面(背面)安装在热通道上,实现冷热气流分隔。

6.2.8 根据机房内散热方式,机架可采用通透式机架或半封闭式机架,应符合以下要求:

1. 通透式机架的前、后门开孔率均不应低于 60%。在安全隔离允许时,可采用前后均无柜门的开架式机柜。

2. 半封闭式机架内的冷空气通道应充分保证制冷效果,应根据风速和机柜散热所需风量计算确定进风口面积,进风口面积宜可调。后门开孔率应不低于 60%。

3. 在安装架内主设备时,尺寸较深的设备或者正面线缆较多的设备,应尽量安装在远离进风口的一端。当机架内未装满设备时,未安装设备的位置前部应统一安装挡风盲板(假面板)。

6.2.9 IDC 主机房区内通道与机架列间距应符合以下要求:

1. 设备机架列间距应考虑工艺设备维护空间、用户安全隔离需求,还应根据机架装机功率密度的大小,合理选择列间距。

2. 当 IDC 机房采用通透式机架时,冷通道间距应根据区域机柜功率密度核算,一般可为 1 200~1 800 mm。热通道间距宜为 900~1 200 mm。

3. 当 IDC 主机房区采用半封闭式机架时,机架列间距宜为 900~1 200 mm。

4. 成行排列的机架,其长度超过 6 m 时,两端应设有出口通道;当两个出口通道之间的距离超过 15 m 时,在两个出口通道之间还应增加出口通道。主通道的宽度不宜小于 1.5 m,次通道的宽度不宜小于 1 m。

6.2.10 主机房内机架宜采用统一颜色,机架前后门样式宜统一。各列机架高度、同一列机架宽度和深度宜统一。对于非标准机架,宜设置非标准区域放置。

6.2.11 宽度等于 600 mm 的机架,宜采用单开门方式;宽度大于 600mm 的机架,宜采用双开门方式。

6.2.12 机架内应采用集成布线通道,以便于布设、管理大量缆线。数据线和电源线宜布设在机架上方并应存储在机架背面,以便于维护和管理。缆线管理应避免电源线和数据线妨碍排出气流。

6.2.13 机架的安装设计应符合 YD 5059《电信设备安装抗震设计规范》的各项规定,按所要求的抗震加固措施进行加固。

6.3 电气、空调、布线与安防

6.3.1 IDC 机房供电应符合以下规定:

1. IDC 机房供电设计应符合 YD/T 1051《通信局(站)电源系统总技术要求》和 YD/T 5040《通信电源设备安装工程设计规范》等规范的规定,机房其他电气设计应符合 GB 50174《电子信息系统机房设计规范》和 YD 5003《通信建筑工程设计规范》的规定。

2. 市电供电条件应符合表 6.3.1 的要求。

表 6.3.1 市电供电条件

IDC 级别	A	B	C
市电供电条件	一类	不低于二类	不低于二类

3. IDC 机房内采用的 UPS 供电系统从输入配电设备开始到输出配电都应无单点故障。

6.3.2 IDC 机房空调应符合以下规定。

1. IDC 主机房空调设计应符合 GB 50019《采暖通风与空气调节设计规范》的规定。

2. IDC 主机房区的空调系统应采用大风量、小焓差的机房专用空调,空调机应设不低于 GB/T 14295 规定的粗效 2 类空气过滤器。IDC 主机房空调室内机的配置数量应计算确定,应按不少于总制冷量的 15%~20%考虑备用。

3. IDC 主机房空调送风方式可选择下送风方式或上送风方式。A 级和 B 级 IDC 应采用下送风方式,C 级 IDC 宜优选下送风方式。

4. 选用上送风方式的机房专用空调,布置上送风风管,空调送风口对应机柜冷通道,回风口设置在热通道上。

5. 选用下送风方式的机房专用空调,在机房内设置架空地板,地板高度应随机房内单机柜功耗的进行计算确定。空调冷风在架空地板下通过冷通道上设置的开孔地板(送风口)和机柜前门进入机柜内,空调回风口设置在热通道上。空调冷风也可通过半封闭式机架内的进风口送风。

6. 单机架平均运行功率大于 10kW 的局部机架区域,可在原有送风方式的基础上增设辅助制冷设备。

6.3.3 IDC 机房综合布线应符合以下规定。

1. IDC 机房综合布线应符合 GB 50311《综合布线系统工程设计规范》。

2. IDC 各机房(区)应根据功能要求划分成若干布线区域,包括网络接入间(区)、主配线区域、水平配线区域、区域配线区域和设备配线区域。

3. IDC 主机房区配线子系统的信息点规模应根据 IDC 自有系统及出租/托管业务机房(区)的业务规模确定。

4. 根据配线需求合理配置列配线柜和总配线柜。

5. 机房线缆布放应采用上走线的方式,线缆布放时应采用走线架,走线架应选择开放式线架,宜设置二层走线架。

6. 走线架应整体规划,整体走线架设施应不影响机房空调气流组织。走线架及走线槽道的安装设计应符合 YD/T 5026《电信机房铁架安装设计标准》和 YD 5059《电信设备安装抗震设计规范》的各项规定。

6.3.4 IDC 机房的安全防范应符合以下要求。

1. IDC 机房安全防范等级为一级。

2. IDC 机房应设置安全防范监控系统。安全防范系统应由视频安防监控系统、出入口控制系统等子系统组成。各系统的设计应符合 GB 50348《安全防范工程技术规范》和 GB/T 50314《智能建筑设计标准》。

6.3.5 IDC 机房宜配置集成的环境和设备监控及能源管理系统,对机房环境、水浸、供电和空调系统工作参数与状态、机架供电情况等等进行实时监控、统计。

7 网络子系统

7.1 网络结构

7.1.1 IDC 网络架构应采用层次化、模块化的设计方式,整个网络可分为四层:互联网接入层、汇聚层、业务接入层和运维管理层,共同构成 IDC 的网络子系统,如图 7.1.1 所示。

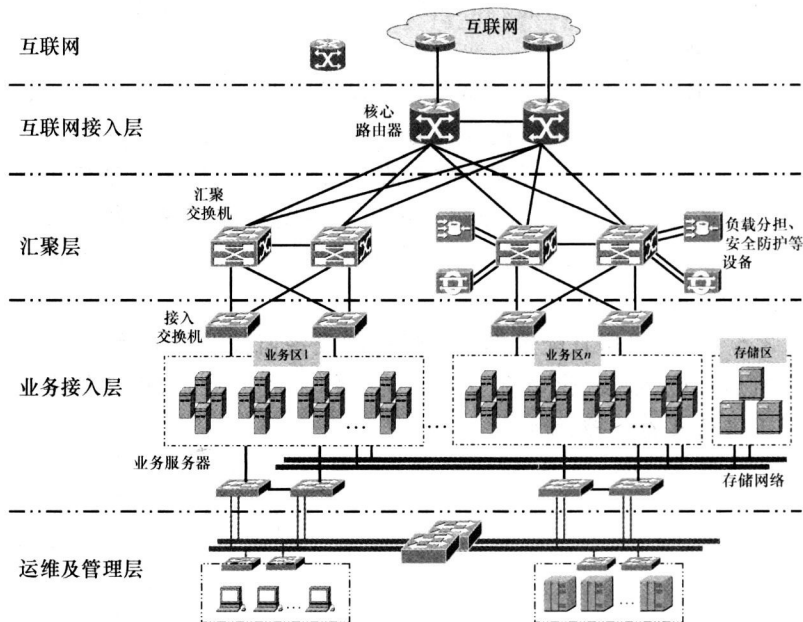


图 7.1.1 IDC 网络结构示意图

1. 互联网接入层应配置核心路由器实现与互联网的互联,对 IDC 内网和外网的路由信息进行转换和维护,并连接汇聚层的各

汇聚交换机,形成 IDC 的网络核心。

2. 汇聚层应配置汇聚交换机实现向下汇聚业务接入层各业务区的接入交换机,向上与核心路由器互联。部分流量管理设备、安全设备可部署在该层。大客户或重点业务可直接接入汇聚层交换机。

3. 业务接入层应通过接入交换机接入各业务区内部的各种网络设备、服务器设备、存储设备等。

4. 运维管理层宜独立成网,与 IDC 业务网络进行隔离,通过运维管理层的接入及汇聚交换机连接管理子系统各种设备。

5. 对于 C 级 IDC 中规模较小的,互联网接入层和汇聚层可合设。

7.1.2 IDC 网络结构中互联网接入层与外部互联网、互联网接入层与汇聚层、汇聚层与业务接入层之间的拓扑结构应无单点故障。

7.1.3 互联网接入层至少配置两台核心路由器,核心路由器与互联网连接应符合下表 7.1.3 的规定。

表 7.1.3 核心路由器与互联网连接

IDC 级别	A	B	C
核心路由器 与互联网连接	宜与互联网省际骨干网核心汇接节点连接,至少与 1 个节点的两台不同设备连接,或者与 2 个不同节点连接	宜与互联网省内骨干网核心汇接节点或与城域网出口节点连接,至少与 1 个节点的两台不同设备连接,或者与 2 个不同节点连接	宜与互联网省内骨干网节点或与城域网出口节点连接,至少与 1 个节点的两台不同设备连接
连接带宽	应根据业务需求估算确定,不宜小于 10 Gbps	应根据业务需求估算确定,不宜小于 10 Gbps	应根据业务需求估算确定,不宜小于 1 Gbps

7.1.4 根据业务需求,防火墙、负载均衡器、IDS、IPS、审计系统等安全系统和流量管理系统可设置在汇聚层。

7.1.5 业务接入层应采用模块化设计,进行区域划分。根据业务经营者提供的业务种类,可将业务接入层从逻辑上分为不同的业务网络区域,包括主机托管区、主机租用区、VIP 用户区、集团用户区、增值业务区等。

7.1.6 汇聚交换机和接入交换机的数量配比、接入交换机连接的业务服务器数量应合理确定。

7.1.7 运维管理层应进行区域划分,可包括客户操作区、客户远程接入区、管理子系统区等。

7.2 路由

7.2.1 IDC 可作为一个单独的自治域,采用 BGP 与互联网连接,也可不作为单独自治域采用 OSPF 或 ISIS 协议与互联网连接。

7.2.2 互联网接入层核心路由器应对内部路由信息进行聚合后向互联网发布,互联网接入层核心路由器应向 IDC 内部网络发布默认路由信息,不宜发布来自互联网的具体路由信息。

7.2.3 IDC 内部网络路由可设计成二/三层混合方式或大二层方式,应符合以下要求:

1. 采用二/三层混合方式时,IDC 内部路由协议宜选择 OSPF。宜采用 OSPF 双层次多区域配置方式,互联网接入层核心路由器组成核心 OSPF 区域,汇聚交换机和接入交换机组成多个 OSPF 二级区域。

2. IDC 提供云计算服务时,宜采用扁平的大二层方式,内部网络采用二层组网。

8 资源子系统

8.0.1 IDC 应通过在业务接入层划分 VLAN 网络,形成不同用户服务的网络资源。

8.0.2 IDC 可在业务接入层配置业务服务器等设备,形成为用户服务的主机计算资源。

8.0.3 IDC 可在业务接入层建设 SAN 或 NAS 等存储网络,形成为用户服务的存储资源。

8.0.4 IDC 可根据业务经营者的业务规划,通过配置中间件、应用平台环境等有关软件,形成软件应用能力资源。

8.0.5 IDC 可采用云计算技术提高资源使用的灵活性和效率,目前可主要采用虚拟化技术形成 IDC 的计算资源池、存储资源池、网络资源池、应用能力资源池等。

9 业务子系统

9.0.1 在机房设施子系统、网络子系统、资源子系统和管理子系统的支撑下, IDC 应能向用户提供基本业务和可选的增值业务。

9.0.2 IDC 的业务子系统应具备提供分级服务的能力。

9.0.3 在业务经营者建设有多个 IDC 时, 各个 IDC 宜通过互联网联网, 通过 CDN 等技术实现业务内容的合理分布和共享。

10 管理子系统

10.1 系统设置

10.1.1 IDC 的管理子系统宜统一纳入业务经营者的 BSS、OSS 系统中,不独立设置。条件不具备时,IDC 也可单独建设管理及运营支撑系统。

10.1.2 IDC 管理子系统应在 IDC 网络的运维管理层中设置管理用采集服务器设备或代理服务器设备。运维管理层应通过专线或 VPN 与 BSS/OSS 连接。

10.1.3 IDC 宜配置基于 IP 的 KVM 系统。

10.2 网络管理

10.2.1 网管管理的对象应包括 IDC 内自有设备以及提供代维代管类增值业务的用户设备。

10.2.2 网络管理功能可包括设备管理、拓扑管理、配置管理、性能管理、故障管理和统计报表等功能。

10.2.3 设备管理应与被管设备的管理接口相连,提供对各设备基本配置信息的管理。设备管理应支持设备的带内管理和带外管理两种方式。

10.2.4 拓扑管理宜实现以下功能。

1. 支持网络拓扑的自动发现、拓扑结构动态刷新。

2. 提供多视图管理,支持用户自定义视图。提供多种视图模板,按权限可分为管理员视图、客户视图;按精细程度分为节点物理拓扑视图、互联网接入层拓扑视图、汇聚层拓扑视图、业务接入层拓扑视图、运维管理层拓扑视图;逻辑上分为 VLAN 视图、端口

流量视图等。拓扑管理功能宜在视图上提供向其他功能的链接。

3. 对网络设备进行定时(轮询间隔时间可配置)的轮循监视和状态刷新并表现在网络视图上。

4. 支持拓扑过滤,支持快速查找拓扑对象,并在导航树和拓扑视图中定位。

10.2.5 性能管理宜实现以下功能:

1. 监控主机、网络的各性能状态,形成历史记录。

2. 可设置系统侦测参数,包括 SNMP 时延, Ping 的时延、端口服务连接的时延。

3. 提供全网性能分析,包括网络流量、利用率、误码率等性能指标。

4. 提供对交换机、路由器、防火墙、主机等各类管理对象持续的性能参数采集、分析、存储。

10.2.6 故障管理宜实现以下功能:

1. 提供对性能管理中采集的性能指标的管理,包括告警阈值定义、告警方式定义、实时性能监控等。

2. 提供事件分级功能,将事件分为正常、警告、异常三级。

3. 支持告警拓扑的直观呈现及定位,将显示的焦点定位到产生选定告警的拓扑对象,可包含专门的事件拓扑视图。

4. 支持多种告警方式,包括:声响、颜色、电子邮件、电话、短消息、外部程序等。

5. 提供故障处理的相关报表,可以按时段和灵活的条件组合查询故障,提供故障处理知识库的管理。

6. 应提供常见和实用的网络测试诊断工具集。

7. 支持告警溯源,实现 MAC 地址端口反查和 IP 地址端口反查等。

10.2.7 统计报表宜实现以下功能:

1. 提供各管理对象的性能统计报表。

2. 提供各管理对象的故障统计报表。

3. 可以分析报表数据,对报表数据进行聚合、排序、比较等,并能图示分析结果。

4. 提供日、月、周和年报表。

10.3 资源管理

10.3.1 资源管理应支持对空间位置资源(机房/机架/机位)、IP 地址/带宽资源、存储空间资源、设备资源、应用资源、虚拟基础架构等的管理,应实现资源的日常管理、统计、核对。

10.3.2 空间位置资源管理宜实现以下功能。

1. 可建立、修改、删除机房相关信息,应包含机房地址、面积、负责人联系电话、手机、电子邮箱、机架总数量、各层交换机/路由器端口总数量、出口带宽、IP 范围、IP 数量等属性。

2. 可建立、修改、删除机架、机位相关信息,应包含机架规格、电源个数(已使用个数)、已使用接入层交换机端口个数、可使用机位(按 u 计算)、已使用机位(按 U 计算)、已使用 IP 个数、高度、宽度、深度、机架编号、自用端口等属性。

10.3.3 IP 地址/带宽资源管理宜实现以下功能。

1. 可记录各业务所涉及设备占用或释放的资源信息。

2. 支持对总带宽、已分配带宽、可分配带宽的管理。

3. 支持 IP 地址资源的自动监控报警功能。

10.3.4 设备资源管理宜实现对下述信息的管理:设备 ID 号、设备类型(核心/汇聚/接入层路由器和交换机、服务器、存储设备、防火墙等)、设备名称、设备性质(自有设备、租赁设备、用户设备)、设备型号、尺寸(长、宽、高)、重量、耗电量、发热量、散热方向(前后左右上下)、技术指标(内存、CPU、硬盘)、设备安装存放信息(含括机房、机架、机位)。对于用户设备和租赁设备应说明所属的用户信息(包括用户名称、用户联系方式、用户身份证 ID、设备型号/尺寸大小等)。

10.3.5 存储空间资源管理宜支持对出租划分出的各种等级存储

空间的管理,包括空间容量、访问方式、文件系统、RAID 等级、备份方式、用户信息等。

10.3.6 应用资源管理宜实现对下述信息的管理:应用类型、应用环境、应用信息、应用使用的接口信息、应用使用的系统软件资源和硬件资源、用户信息等,宜支持端口资源的自动监控报警功能。

10.3.7 虚拟基础架构管理宜实现对虚拟网络资源、虚拟计算资源、虚拟存储资源、虚拟应用资源等资源池的生命周期管理和资源调度,实现多种业务需要的调度算法、资源用量监控。

10.4 业务管理

10.4.1 业务管理应实现 IDC 的服务管理和产品管理。

10.4.2 服务管理宜实现对 IDC 服务所包含的所需资源、服务级别、服务承诺、名称、描述和状态等信息的建立、修改、查询、统计等功能。

10.4.3 产品管理宜实现对 IDC 产品所包含的名称、描述、状态、所包含服务种类等信息的建立、修改、查询、统计等功能。

10.5 运营管理

10.5.1 运营管理应提供业务运营、密码管理、权限管理、客户管理、统计分析等功能。

10.5.2 业务运营宜实现以下功能:

1. 实现 IDC 业务的开通、变更和终止。
2. 通过 workflow 系统实现 IDC 业务所需的资源分配、施工和验收。
3. 支持工单查询和统计。

10.5.3 密码管理宜实现以下功能:

1. 统一管理 IDC 的各类密码,对于密码的基本信息(设备或应用系统、人员、账号、密码、时限)进行登记和查询。
2. 对于密码申请和修改,通过 workflow 系统进行申请、批准、分

配的过程管理。

3. 实现密码的生命周期管理,对于即将过期的密码应通知提示。

10.5.4 权限管理宜实现以下功能:

1. 实现用户级别和权限管理。
2. 实现访问控制功能。
3. 提供安全日志,支持审计功能。

10.5.5 客户管理宜实现以下功能:

1. 实现客户服务。
2. 实现客户信息管理。
3. 实现订购关系信息管理。
4. 支持客户关系管理。

10.5.6 统计分析宜实现以下功能:

1. 支持按客户进行统计分析。
2. 支持按业务进行统计分析。

11 网络与信息安全

11.1 安全目标

11.1.1 IDC 应设立明确的安全目标,保护 IDC 的信息资产,根据安全策略控制出入网络的信息流,系统应具有较强的抗攻击能力。

11.1.2 IDC 应对整个系统进行安全域划分,各个安全域根据安全需求确定不同的安全级别、制定不同的安全策略。

11.2 安全技术措施

11.2.1 IDC 网络子系统的各个网络设备应进行安全加固,业务接入层下各业务区内的主机应进行安全加固,包括禁用不必要的服务、修改不安全的配置、利用最小特权原则严格控制对设备的访问、配置适当的软件版本和必要的补丁等。

11.2.2 IDC 互联网接入层应能防范分布式拒绝服务攻击,A 级和 B 级 IDC 宜在 IDC 出入口部署流量清洗系统。

11.2.3 IDC 汇聚层在其下连的业务接入层业务区有需求时,应在汇聚层处配置防火墙、入侵检测系统等安全设备。

11.2.4 IDC 业务接入层应配置病毒防范系统,实现对 IDC 自有设备进行统一管理,并具备对有需求的用户设备进行病毒防范管理的能力。

11.2.5 IDC 业务接入层宜配置网页防篡改系统,实现防范 Web 服务器上的网站页面被非法篡改,且在页面遭受非法篡改后能够自动屏蔽非法网页以及进行页面的自动恢复。

11.2.6 IDC 运维管理层和被管系统的接口处宜配置安全控制网关,实现基于用户名、用户域名的网络权限精确管理、实现用户访

问日志的记录、支持多种口令的认证,实现用户终端审计和用户行为审计。

11.2.7 IDC 应提供安全可靠的 VPN 接入手段,实现 IDC 运维人员、客户维护人员远程访问 IDC 自有及托管设备。

11.3 安全管理

11.3.1 IDC 应独立建设安全管理系统或与经营者的其他安全管理系统合设,实现对 IDC 的各项安全管理功能,并具备向用户提供安全防护类增值业务的能力。

11.3.2 根据 11.2 节各条要求配置的安全设备宜纳入 IDC 安全管理系统进行集中、统一管理。

11.4 备案管理与有害信息监测

11.4.1 IDC 应提供备案管理功能,实现对 IDC 机房中提供互联网服务的站点的备案信息进行管理,备案管理功能的系统实现可与 IDC 管理子系统适当整合,或与经营者的其他备案管理系统集中统一实现。

11.4.2 备案管理实现系统应实现 ICP 备案信息库管理、IP 备案地址库管理、协同处理违法违规网站禁入、统计分析报表管理等功能。

11.4.3 IDC 应在互联网接入层出入口配置应用监控系统,进行 IDC 有害信息监测。IDC 应用监控系统也可与经营者的有关互联网应用监控系统整合实现。

11.4.4 IDC 应用监控系统应能实现有害信息监测、异常邮件行为监测、垃圾邮件过滤、网站内容有效性测试、业务流量统计分析等功能。

11.4.5 IDC 的备案管理与有害信息监测系统实现应支持向有关主管部门上报所要求的数据信息,并根据要求实现与主管部门有关管理系统的接口。

12 计费

12.0.1 IDC 计费应支持资源占用、能力占用、服务使用、业务交易量及其组合等模式。

12.0.2 IDC 应支持灵活的计费类型,支持不同时间段、折扣、套餐等类型。

12.0.3 IDC 计费功能的实现宜与经营者的 BSS 系统统一考虑, IDC 管理子系统应提供计费原始信息。

12.0.4 IDC 的计费记录/话单准确率应不小于 99.999%。

12.0.5 IDC 的计费记录或话单应在线存储不短于 3 个月、离线存储不短于 6 个月。

13 IP 地址与码号

13.1 IP 地址

13.1.1 IDC 的 IP 地址应合理规划、分配,应能便于应用监测、地址聚合和访问控制。

13.1.2 IDC 应具备以双协议栈方式同时支持 IPv4 和 IPv6 的能力。

13.2 码号

13.2.1 IDC 的用户应合理编码,编码规则应便于计费结算和管理,符合有关管理规定。

13.2.2 IDC 自有设备和托管设备应进行合理编码,编码规则应便于维护管理,符合有关管理规定。

14 服务质量

14.0.1 IDC 应符合表 14.0.1 中的服务质量要求。

表 14.0.1 服务质量

IDC 级别	A	B	C
网络可用性	$\geq 99.99\%$	$\geq 99.9\%$	$\geq 99.5\%$
网络时延(从 IDC 用户设备接入端口到互联网接入节点下联端口,ping 测试包大小为 512 字节)	$\leq 3\text{ ms}$	$\leq 5\text{ ms}$	$\leq 10\text{ ms}$
网络丢包率(从 IDC 用户设备接入端口到互联网接入节点下联端口,ping 测试包大小为 512 字节)	$\leq 0.01\%$	$\leq 0.1\%$	$\leq 0.5\%$
客户服务	7×24 小时	7×24 小时	7×24 小时
故障平均修复时间	$\leq 2\text{ 小时}$	$\leq 4\text{ 小时}$	$\leq 6\text{ 小时}$

14.0.2 IDC 应具备向用户提供不同产品分级服务质量的能力。

15 能 耗

15.0.1 IDC 机房应采取充分的节能设计,采用高效节能设备和系统方案,PUE 不宜大于 2。

15.0.2 IDC 应支持对内部各种设备的能耗进行综合管理,可与管理子系统中有关管理功能实现整合。

16 设备配置

16.0.1 IDC 各种主设备和配套设备应本着性能稳定、安全可靠、技术先进、低能耗、兼容性好、经济合理、扩展性强等原则进行配置,近期建设规模与远期发展规划应协调一致。

16.0.2 IDC 中采用的各种设备应符合有关的设备技术规范。

16.0.3 IDC 中的关键设备应具有高可靠性,重要部件负载分担、关键部件热备份,具有故障时自动倒换功能。

16.0.4 IDC 中采用的各种网络设备应具备线速转发能力,具有良好的突发流量缓存能力,支持优先级控制。

16.0.5 IDC 中采用的网络设备、服务器设备、存储设备和有关系统软件、应用软件宜支持虚拟化功能。

16.0.6 IDC 中的网络带宽利用率不宜大于 70%,网络设备、服务器设备、存储设备的忙时 CPU 利用率、内存利用率、吞吐能力和会话处理能力的利用率均不宜大于 70%。

16.0.7 IDC 机房设施子系统的各方面配置应具备能够扩展到支持 IDC 终期规模的能力。

附录 A 本规范用词说明

本规范条文中执行严格程度的用词,采用以下写法。

- A. 0. 1 表示很严格,非这样做不可的用词:
 - 正面词采用“必须”;
 - 反面词采用“严禁”。
- A. 0. 2 表示严格,在正常情况下均应这样做的用词:
 - 正面词采用“应”;
 - 反面词采用“不应”或“不得”。
- A. 0. 3 表示允许稍有选择,在条件许可时首先应这样做的用词:
 - 正面词采用“宜”;
 - 反面词采用“不宜”。
- A. 0. 4 表示允许有选择,在一定条件下可以这样做的用词,采用“可”。

引用标准名录

GB 50019	采暖通风与空气调节设计规范
GB 50174	电子信息系统机房设计规范
GB 50311	综合布线系统工程设计规范
GB 50348	安全防范工程技术规范
GB 50367	混凝土结构加固设计规范
GB/T 14295	空气过滤器
GB/T 50314	智能建筑设计标准
YD 5003	通信建筑工程设计规范
YD 5059	电信设备安装抗震设计规范
YD/T 1051	通信局(站)电源系统总技术要求
YD/T 1821	通信中心机房环境条件要求
YD/T 5026	电信机房铁架安装设计标准
YD/T 5040	通信电源设备安装工程设计规范

中华人民共和国通信行业标准

互联网数据中心(IDC)工程设计规范

Design Specifications for
Internet Data Center Engineering

YD 5193—2014

条文说明

编写说明

互联网数据中心(IDC)是以电信级机房和网络资源为依托,以高水平专业化技术支撑队伍为基础,为各类用户提供各种资源出租以及相关增值业务的一种电信服务。IDC 拥有完善的设备(包括高速互联网接入带宽、高性能网络、安全可靠的机房环境等)、专业化的管理、完善的应用级服务平台。随着电信行业全业务运营的发展,互联网业务与其他电信业务不断融合发展,同时随着各行业信息化工作的不断深入,电信运营商和各种企事业单位对互联网数据中心的业务需求越来越强烈,互联网数据中心的建设规模不断扩大。

《互联网数据中心(IDC)工程设计规范》主要规定了 IDC 的业务、系统组成、IDC 分级、机房设施子系统、网络子系统、资源子系统、业务子系统、管理子系统、网络与信息安全、计费、IP 地址与码号、服务质量、能耗、设备配置等,强调了 IDC 机房应采取有利的节能设计,采用高效节能设备和系统方案,并根据 IDC 机房的级别对能源利用率提出了不同的要求。

规范对 IDC 的系统组成进行了模型抽象,提出 IDC 应包含机房设施子系统、网络子系统、资源子系统、业务子系统、管理子系统五大逻辑功能部分。其中:

机房设施子系统为 IDC 提供机房、供电、消防、空调、安防、布线等系统;

网络子系统为资源子系统和业务子系统提供网络环境;

资源子系统为业务子系统提供开展业务运营所需的基础资源池,包括计算资源、存储资源、网络资源、软件应用能力资源等;

业务子系统提供 IDC 的基本业务和增值业务;

管理子系统为 IDC 的运营维护提供必要的管理支撑,包括网络管理、资源管理、业务管理、运营管理、安全管理等。

规范中对于每个子系统提出了详细的技术要求。在总结当前最佳实践的基础上,重点在机房设施子系统一章中充分应用了各种节能措施,同时在规范中提出了能源利用效率(PUE)指标的要求。

规范还提出了服务质量指标要求和安全方面的具体要求。

该规范的制定可以规范互联网数据中心的工程设计,提高设计的标准化程度,保证对用户的服务质量,促进新技术及节能措施在工程设计中的应用以及提高网络安全性。该规范的提出符合落实科学发展观的要求,符合国家有关资源节约与综合利用等方针政策的规定。

目 次

1	总则	39
3	业务	40
4	系统组成	42
5	IDC 分级	43
6	机房设施子系统	44
6.1	机房要求	44
6.2	机架要求	44
6.3	电气、空调、布线与安防	45
7	网络子系统	46
7.1	网络结构	46
8	资源子系统	47
10	管理子系统	48
10.1	系统设置	48
10.2	网络管理	48
10.3	资源管理	48
10.4	业务管理	48
10.5	运营管理	49
11	网络与信息安全	50
11.1	安全目标	50
11.2	安全技术措施	50
11.4	备案管理与有害信息监测	51
13	IP 地址与码号	52
13.2	码号	52
15	能耗	53
16	设备配置	55

1 总 则

1.0.1 互联网数据中心(IDC)是以电信级机房和网络资源为依托,以高水平专业化技术支撑队伍为基础,为各类用户提供各种资源出租以及相关增值服务,并定期向用户收取相应服务费用的一种电信服务。IDC 拥有完善的设备(包括高速互联网接入带宽、高性能网络、安全可靠的机房环境等)、专业化的管理、完善的应用级服务的服务平台。

1.0.2 IDC 系统网络在设计时,应在进行多方案技术经济比较的基础上,实现高可靠性、平滑的可扩展性、良好的安全性。系统应符合相关技术标准、规范的规定。系统设计应与业务和网络发展规划相适应,可以近期业务需求为主,兼顾远期业务发展。

1.0.3 本条款编写依据是《中华人民共和国电信条例》第五十四条规定:“国家对电信终端设备、无线电通信设备和涉及网间互联的设备实行进网许可制度。接入公用电信网的电信终端设备、无线电通信设备和涉及网间互联的设备,必须符合国家规定的标准并取得进网许可证。实行进网许可制度的电信设备目录,由国务院信息产业主管部门会同国务院产品质量监督部门制定并公布施行”。

1.0.4 本条款编写依据是《中华人民共和国防震减灾法》中有关新建、扩建、改建工程应当达到抗震设防要求的内容。通信系统工程作为生命线工程,建设中使用的主要电信设备必须满足抗震设防的要求,以提高网络的抗震设防水平。

3 业务

3.0.1 IDC 的基本业务主要属资源出租型。主要业务的含义如下。

1. VIP 机房出租:指 IDC 根据用户需要,向用户提供封闭或半封闭的空间放置用户自备的网络和服务器等设备,管理和配置多由用户独立完成。VIP 机房配备独立的门禁系统,在网络出口方面可共用 IDC 的互联网出口,也可使用 IDC 提供的专线出口。

2. 主机托管:指 IDC 为用户提供一定的“空间”和“带宽”,其中“空间”是参照机架服务器的规格选取一定的机架或机位空间,用户将自己的网络设备、服务器托管在租用的空间内。用户拥有对托管设备的所有权和完全控制权限,用户自行安装软件系统和自行维护。

3. 机架出租:指 IDC 向用户提供一定数量的机架,用户的机架可自行安装、维护自备设备。根据用户需求,机架可与其他机架之间采用通透式钢笼隔离。

4. 服务器出租:指 IDC 规模采购服务器设备,出租给 IDC 用户,并向承租人提供主机的硬件维修、保养等服务。用户拥有对租用设备的使用权和完全控制权限,自行安装和维护软件系统。

5. 虚拟机出租:把一台运行在互联网上的服务器资源(系统资源、网络带宽、存储空间等)按照一定的比例划分成若干台“虚拟”的“小主机”,每一个虚拟主机都具有独立的域名,常用于放置一个网站的网页、图片、数据库等内容,只能实现 HTTP、FTP、E-mail 等基本的互联网服务。同一台服务器上的不同虚拟主机是彼此独立的,并可由用户自行管理。

6. 带宽出租:指 IDC 可根据用户的需要提供不同形式的端口

接入方式和接入带宽,根据接入方式的不同分为共享型、独享型。共享型指一定数量的用户租用某种网络端口并共享同等级出口带宽,多台用户设备共同接入 IDC 接入层交换机,通过该交换机同一条上行链路接入 IDC 网络汇聚层设备,用户带宽受该链路所带用户数影响;独享型指用户租用某种网络端口并独享出口带宽,用户设备直接接入 IDC 汇聚层或核心层交换机,独占汇聚层或核心层设备的一个端口,并完全占用该出口带宽,IDC 为用户提供受保障的带宽。

7. IP 地址出租:指在上述业务中,IDC 宜向用户提供一定数量的 IP 地址,在用户需要额外数量的 IP 地址时需另行租用。

3.0.2 IDC 的增值业务大多属能力服务型,可由用户选购,一些服务含义如下。

1. 在线备份:为用户提供本地重要数据的网络存储备份服务,在发生故障时对系统进行快速自动恢复。

2. 负载均衡:通过负载调度技术,将大量的并发访问或数据流量分担到多台节点设备上分别处理,减少用户等待响应的时间,提高设备的利用率。

3. 设备代理监测:为用户提供网络状况和系统运行状况的实时监测,向用户提供用户网络系统运行数据、网络流量报表和网络性能分析等。

4. 设备代理维护:由专业维护人员为用户提供托管设备的日常维护。

5. 远程维护:远程仿真键盘、视频、鼠标,实现用户远程对所托管或租用设备的控制。

6. 系统集成:为用户定制系统建设集成方案,提供方案实施和设备安装调试等服务。

7. 基于云计算概念提供的服务将成为 IDC 发展的新模式。云计算是一种服务、新的商业模式,也有其技术特点。根据提供的服务类型,目前可将云计算服务分为三类:IaaS、PaaS、SaaS。

4 系统组成

4.0.1 各子系统含义补充说明如下。

机房设施子系统指为 IDC 运营所提供的一系列基本配套设施,主要为供电系统、消防系统、空调系统、安防系统、布线系统、照明系统等。

网络子系统由路由器、交换机等数据通信设备和安全设备等组成。网络子系统是开展 IDC 业务运营的基础,对外担负着 IDC 与外部互联网的互联互通功能,对内承载着各种 IDC 业务系统。安全设备部署在 IDC 各网络层内,防范 IDC 来自外部互联网的攻击以及保障 IDC 内部网络和业务的正常运行。

资源子系统是 IDC 用来开展业务运营的基础,包括计算资源、存储资源、IP 资源、带宽资源、机房空间资源等资源。业务通过各种资源的合理搭配来为 IDC 客户提供服务。

业务子系统是 IDC 的核心要素,也是 IDC 价值的具体表现形式。它根据市场需求,将 IDC 内的各种资源进行合理的整合和配置,对外包装出符合市场需求的可运营产品或服务,并将这些产品和服务销售给 IDC 客户。

管理子系统为 IDC 的稳定运行和业务运营提供必要的各种支撑服务。

5 IDC 分级

5.0.1 IDC 机房的分级综合参考了国家标准 GB 50174《电子信息
系统机房设计规范》和 TIA/EIA—942。在国家标准 GB 50174《电
子信息系统机房设计规范》中,将机房分为 A、B、C 三级;在 TIA/
EIA-942 中,将数据中心分为一级到四级,但是一级基本没有规定
冗余可靠性要求。因此本规范规定了三级 IDC 的分级要求。

IDC 的分级不仅与技术有关,还应与运维管理能力、服务能力
等管理、运营因素相关,本规范主要涉及有关技术要求。经营者应
对 IDC 进行服务等级评审,规范机房分级服务规范,完善营销组织
管理和服务支撑保障,建立相对统一的客户响应机制。

5.0.2 IDC 级别的确定主要根据 IDC 内所装业务系统的重要性
确定。例如,面向多省或全国提供业务的 IDC,其所装业务系统的
中断将影响多省或全国,属重大影响,因此应为 A 级。面向全省提
供业务的 IDC,其所装业务系统的中断将影响全省,属较大影响,因
此可为 B 级。

仅面向本地市区域提供业务的 IDC,其所装业务系统的中断将
仅影响本地,影响一般,可为 C 级。

6 机房设施子系统

6.1 机房要求

6.1.1 本规范 6.2.7 条要求 A 级和 B 级 IDC 主机房形成冷、热通道,但现有规范未按照冷热通道的不同规定机房环境温度要求。考虑到不断用节能减排技术,在 IDC 工程实施中,应积极研究冷热通道的不同温度范围要求。

6.1.2 IDC 机房不宜选在市中心、商业区等繁华地区。

6.1.3 IDC 主机房区中,网络子系统机房(区)主要用于安置 IDC 网络子系统的各种传输设备、数据网络设备和配线设备等;资源子系统机房(区)主要用于安置 IDC 资源子系统的各种服务器设备、存储设备等;管理子系统机房(区)用于安置 IDC 管理子系统的各种设备;出租/托管业务机房(区)用于向用户提供各种机房空间或机位。

6.1.7 工艺生产要求的净高(2 500~3 000 mm)=机架高度(2 000~2 200 mm)+走线架高度(400~600 mm)+机架与走线架间隔高度(100~200 mm)。当机房进深过大时,需进一步考虑设置热风的回风管道的高度要求。

6.2 机架要求

6.2.2 采用高密度机架方案可以节省能耗、节约投资。但是局部过大的运行功率将对机房散热带来过高要求。在机房内供电和制冷条件允许的情况下单机架采用更高运行功率时,局部单机架平均运行功率建议最大不超过 30 kW/架。

6.2.3 机架内的每个电源分配模块分别设置供架内设备取电的

分路空气开关,机架每路电源分配模块的负载能力宜相同。机架从机房内电源分配柜或列头柜引接两路独立电源至机架内电源分配模块,形成不同供电回路,架内设备的不同电源模块分别接入不同电源分配模块的分路空气开关。

6.2.7 机房的冷热通道组织可以实现冷热气流分隔,形成良好的气流组织,以提高空调的制冷效率。

6.2.8 半封闭式机架的前门与架内安装的设备(或假面板)之间设置专用冷空气通道,前门封闭、后门开孔。机房采用下送风方式时,半封闭式机架底板前部(机架前门与设备间)设置一独立进风口。

尺寸较深的设备或者正面线缆较多的设备要求尽量安装在远离进风口的一端是为了避免阻挡冷气流动。

6.3 电气、空调、布线与安防

6.3.2 下送风方式包含了机房下送风和机柜下送风两种方式。对应机架散热方式,机房下送风时采用通透式机架,机柜下送风时采用半封闭式机架。

6.3.3 走线架设施不影响机房空调气流组织的做法,如列走线架尽量安装在机架上方,不应安装在热通道上方等。

6.3.4 IDC 机房的视频监控摄像头要分布合理、监控全局、避免死角。

7 网络子系统

7.1 网络结构

7.1.1 IDC 网络结构采用了前端业务网络与后台管理网络分离、层次化、模块化设计方式。运维管理层和业务网络物理隔离的设计方法优点如下。

1. 即使业务网络遭受攻击,也可以正常通过管理网络对设备进行管理,为其提供服务,快速诊断问题,以减少业务损失。

2. 管理网络的网管、防病毒、漏洞扫描等应用和管理人员的操作均独立于业务网络,对业务网络不产生影响。

3. 维护人员和客户可通过 VPN 远程接入管理网络,通过互联网随时随地实现对 IDC 内网设备的管理。根据业务的发展情况,网络系统可分步建设、灵活扩展,同时也可根据 IDC 业务发展变化的情况,调整业务模块的用途。

7.1.5 业务接入层的区域划分可以采用功能聚类方法进行,可根据用户需求的不同进一步细分。例如对于主机托管区,功能区域一是通过普通接入(不需要经过防火墙)连接到互联网。用户拥有自己的业务设备,用户仅需要从 IDC 租用固定带宽和机位机架的服务;功能区域二通过防火墙、IDS 等安全设备连接到互联网,用户需要使用 IDC 提供的增值服务设备,例如:防火墙、负载均衡设备等;功能区域三通过防火墙、IDS 等安全设备连接到互联网,并提供专线接入服务。

8 资源子系统

8.0.5 云计算可以实现按需动态提供服务,能够通过资源池化充分利用系统资源,克服“资源孤岛”导致的性能过剩,系统繁忙时可动态增加 CPU/内存,系统空闲时回收系统资源,实现资源动态按需索取。利用虚拟化技术,可对计算资源进行整合,实现计算、内存等资源按业务需求进行分配,从而实现如下优势。

1. 提高服务器利用率:整合服务器资源,通过虚拟化技术和资源动态分配技术,让服务器资源没有“闲置”,提高资源利用率。

2. 提升 I/O 性能:通过建立“云存储”,可以实现 I/O 性能的提升。

3. 提高资源易扩展性:资源可按需平滑扩容,扩容时易于实现对现有在运行业务的透明性,通过自动化管理实现新增节点“即插即用”。

4. 提高业务连续性:通过虚拟服务器之间的高可用性功能,提高业务可用性,降低运维成本。

5. 降低管理维护成本:可通过统一管理界面对所有资源进行集中管理和调配,节点之间易于实现容错和故障自愈功能,节约运维管理成本。

6. 节能:通过对闲时负载较小的服务器自动进行负载迁移、休眠、远程唤醒等操作,以节约能源的消耗。

10 管理子系统

10.1 系统设置

10.1.1 IDC 的后台维护工作需要与 IDC 的日常运营工作紧密结合。从 ITIL 角度来看, IDC 在运维监控方面需要建立事件管理、问题管理、变更管理, 并完善资源库等。

10.1.3 配置 KVM 系统便于 IDC 的维护。通过 KVM 系统, IDC 的维护工程师和客户在任何时间、任何地点都可对设备进行 ROM/BIOS 级别的维护。KVM 系统一般由 KVM 交换机、KVM 认证服务器和服务器模块组成。服务器模块与被管设备串口相连, 将信号转换成 IP 信号, 并通过以太网与 KVM 交换机相连。

10.2 网络管理

10.2.6 常见实用的网络测试诊断工具集包括: Ping、TraceRoute、DNS Lookup、路由表、ARP 等来获取。

10.3 资源管理

10.3.3 当系统中 IP 地址资源的状态与实际在线状态不符合时, 应告警确认。

10.3.6 当系统中端口资源的状态与实际在线状态不符合时, 应告警确认。

10.4 业务管理

10.4.1 IDC 业务的基本单位是服务, IDC 产品由一个或多个服务组合而成。

10.5 运营管理

10.5.2 在业务实施过程中,需注意登记各项工作步骤的内容、执行人、执行时间和备注。业务终止前应确认客户没有欠费,业务终止后应释放业务所占用的资源,如机房、机架、IP 地址等。

10.5.4 权限管理指应对 IDC 客户和系统维护人员设置相应的访问控制策略,以及对 IDC 客户和系统维护人员日常操作的管理,以保证系统的安全运行。

11 网络与信息安全

11.1 安全目标

11.1.1 IDC 应保护重要应用、主机和关键服务器,实现信息资产的安全防护,防止非授权的访问和病毒的扩散、防止黑客入侵、防范垃圾邮件、网页篡改、打击网站仿冒等。

11.2 安全技术措施

11.2.2 分布式拒绝服务攻击(DDoS)分为带宽消耗型攻击(大流量攻击)和主机资源消耗型攻击。带宽消耗型攻击会对 IDC 出口造成流量压力,阻塞 IDC 业务网络,影响 IDC 业务运行。主机资源消耗型攻击使服务器处理大量并发攻击请求,严重影响服务器内存、数据库、CPU 的处理性能。

流量清洗系统的实现可由检测子系统和清洗子系统两部分组成。可以在 IDC 出口链路上部署流量检测子系统,检测子系统检测到异常流量攻击后,上报清洗子系统并把受攻击的主机流量引入清洗子系统进行异常流量清洗,并将清洗后的正常业务流量重新注入网络中。

11.2.7 IDC 的 VPN 接入方式可分为 IPSec VPN 和 SSL VPN 两种。IPSec VPN 在 IP 层通过加密与数据源验证,保证数据包在互联网上传输时的私有性、完整性和真实性。SSL VPN 基于标准 TCP/UDP,不受 NAT 限制,能够穿越防火墙,用户在任何地方都能用标准的浏览器通过 SSL VPN 网关代理访问内网资源。

11.4 备案管理与有害信息监测

为落实工业和信息化部《关于进一步加强电信市场准入和年检环节信息安全专项审查的通知》(工信部保[2009]10号)要求, IDC 在提供互联网接入服务和信息服务的时候,需建设接入单位备案管理系统和网站有害信息检测过滤系统。有关功能应符合工信部《接入服务提供者互联网站备案管理功能要求第 1 部分:备案管理系统功能》的要求和《互联网站备案管理工作细则》等的要求。

13 IP 地址与码号

13.2 码号

13.2.2 一种设备编码规则为:设备代码由五部分组成,第 1、2 位为 IDC 业务标识;第 3~5 位为该 IDC 机房所在省的省代码;第 6、7 位为该省的 IDC 机房序号;第 8、9 位为 IDC 机房设备类型;第 10~14 位为该设备序号。

15 能耗

15.0.1 采用能源利用效率(PUE)作为机房整体能效的衡量指标。

PUE 的计算公式为: $PUE = \text{机房总耗电} / \text{主设备耗电}$ 。

其中,机房总耗电是维持机房正常运行的所有耗电,主设备耗电包括各类服务器、存储和网络设备的耗电。

在 IDC 整体系统网络设计中,应从机房、供电、散热、机房布局、设备选型等多个方面考虑降低能耗。节能措施可主要考虑以下几个方面。

1. 设计节能

减少不必要的器件及共享设计。在设备设计时应尽量减少不必要的器件引起的耗电,通过基础部件共享降低系统功耗、减少耗材、减少占地面积。

提高系统集成度,降低单位器件的能源功耗,如采用低能耗芯片,采用固态硬盘等。

2. 运行节能

CPU 变频技术。采用设备在低负荷运行时 CPU 自动降频、服务器闲时可休眠等方式,根据系统负荷自动调节处理器频率,降低设备在低利用率情况下的能源消耗。

分层存储技术。分层存储技术主要是通过将不经常使用的数据由原来高成本低容量的 FC 盘转移到低负载循环高容量的 SATA 盘上,以减少物理磁盘数量,提升能源效率。

设备共享。主要通过设备共享提升设备使用率,多个系统实例共享物理基础设施(电源、冷却),以提高能源的使用效率,减少物理设备的数量,使得动态资源管理成为可能,有效降低机房

热点。

3. 配套节能

减轻设备重量。主要包括单机柜本身的重量、设备机框重量、拉手条重量、设备单板重量的减轻等。

4. 机房及设备热管理

机房保温隔热,优化机房布局,设备分冷热分区放置,增加风扇加大风量,降低局部热点;提高机柜门开孔率,提高散热效率;在机柜内回风通路上增加挡风盲板,以减少机柜后部热风回流到机柜前部,降低机柜入风口温度等。

5. 用电测量与评估

需建立合理的用电测量与评估机制,以便及时、准确及全面了解机房主设备、配套设备等各部分的用电情况,评估机房能源利用效率,发现影响能效的主要问题,并在机房节能方案实施后对节能效果进行评估。

16 设备配置

16.0.1 主设备包括:IDC 网络设备,如核心路由器、汇聚交换机、接入交换机等;IDC 安全设备,如流量清洗系统、防火墙、入侵检测系统、VPN 网关、防病毒系统、用户接入审计系统等;负载均衡、SSL 加速等设备;IDC 服务器/存储设备,如机架服务器、刀片服务器、分布式存储、SAN 存储等;管理子系统的各种设备等。

配套设备包括:机房设施子系统所涉及的专业设备,如消防系统、安防系统、电源系统、空调系统、机架、布线系统等包含的设备,以及相配套的监控管理设备等。

16.0.3 对关键设备的高可靠性要求是为了充分保证系统能够不间断地运行。