

H3C

新一代网络建设 理论与实践

杭州华三通信技术有限公司 著



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

<http://www.phei.com.cn>

新一代网络建设理论与实践

杭州华三通信技术有限公司 著



电子工业出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书面向IP网络技术领域的相关从业者,围绕“新一代网络”对网络技术、网络应用等带来的影响,从“新一代网络”所覆盖的数据中心、广域网、城域网、园区网、无线、安全、管理以及新技术等领域进行详细阐述,可以帮助读者及时掌握网络相关领域的技术与应用变化趋势和应对方案。对从事互联网研究的专家学者及相关企业IT管理者具有重要的参考价值。

未经许可,不得以任何方式复制或抄袭本书的部分或全部内容。
版权所有,侵权必究。

图书在版编目(CIP)数据

新一代网络建设理论与实践/杭州华三通信技术有限公司著. —北京:电子工业出版社, 2011.10

ISBN 978-7-121-14581-0

I. ①新… II. ①杭… III. ①计算机网络—建设—文集 IV. ①TP393-53

中国版本图书馆CIP数据核字(2011)第185791号

责任编辑:赵 娜

特约编辑:王 纲 逯春晖

印 刷:北京天宇星印刷厂

装 订:三河市皇庄路通装订厂

出版发行:电子工业出版社

北京市海淀区万寿路173信箱 邮编 100036

开 本:787×1092 1/16 印张:41.5 字数:1056千字

印 次:2011年10月第1次印刷

定 价:188.00元

凡所购买电子工业出版社图书有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系,联系及邮购电话:(010) 88254888。

质量投诉请发邮件至zlt@phei.com.cn,盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线:(010) 88258888。

序

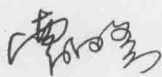
20世纪末以来是互联网发展最快的时期，诞生了Google、Facebook、Twitter、百度、腾讯、阿里巴巴等一个个互联网的传奇。作为后端承载的网络也发生了日新月异的变化，H3C作为网络技术产品和解决方案的领先供应商，与客户一起见证了这个伟大的发展过程，帮助客户走在了信息网络建设的前列。

互联网技术的高速发展带来信息的爆炸式增长，随着越来越多的信息和应用集中在云端，越来越多的终端用户需要及时获得这些信息和应用，建设一个更大容量、自动化、虚拟化、高品质无损传递和绿色节能的网络成为IT网络界共同的呼声。

为了帮助广大客户更加全面地理解新一代网络建设的特点，我们整理了当前在IP网络技术各个领域的创新理论及热点技术，并结合多年来和广大客户的最佳实践经验，推出了这本《新一代网络建设理论与实践》。期望本书能够对广大客户提供有益的参考，并与我国网络技术从业者分享我们的创新知识与实践经验。也期待着大家对我们的产品技术和解决方案提出更好的建议，共同迎接新一代网络大发展的机遇和挑战。

关于本书，我还要感谢那些在IP网络技术领域孜孜不倦地耕耘的华三工程师们，是他们的辛勤与奉献才使得我们始终站在网络技术发展的潮头。我们有理由相信，他们还会给中国网络技术领域带来新的惊喜。

杭州华三通信技术有限公司
副总裁兼首席技术官



· 前 言 ·

经过20年左右的发展，互联网在规模、连接对象和承载的应用等方面都发生了巨大的变化。对于终端用户而言，互联网都是透明且极其简单的。大家都习惯了在电脑上输入一个信息，网络就将它送到接收端。很少有人关心数以亿计的用户连接到庞大的互联网上，网络如何有效将信息传递到对方端的。但作为网络技术、产品和解决方案的开发者，我们必须清醒的意识到技术革新的大幕已经拉开，“新一代网络”从技术、产品准备度和解决方案角度展现到我们面前。

数以亿计的用户每天都在Google和百度上进行信息搜索，在亚马逊、淘宝上购物，通过MSN、腾讯进行即时沟通，或通过Facebook、Twitter形成新的社交关系。当一个具体应用的用户群是数以亿计时，就需要有一种全新的计算方式可以把数以亿计的信息输入进行有效计算并及时输出。现在很多客户需要把几百台、数千台服务器集群为一个计算单元，服务于特定的互联网应用，已经出现超过3000台服务器的集群要求。当这种集群变得极其庞大，我们突然发现在互联网的“心脏”——数据中心，网络连接的对象已经不再是单台服务器或计算机，而是由几百台、数千台服务器互联协同起来的庞大集群计算单元。同时，集群服务器本身，包括硬件、操作系统、数据库有异构性，为了使异构的系统同构并提高单台服务器的计算能力，一台服务器往往又被虚拟化，变成多台虚拟服务器。多台虚拟服务器可以在不同的物理服务器上灵活地进行复制和迁移。虚拟设备既有比一台物理服务器计算能力小的（1:N），也有数百数千台物理或虚拟服务器集群起来的（N:1）。无论1:N还是N:1，都标志着网络的重心开始由物理设备互联的能力向虚拟设备互联的能力进行转移。

新一代网络的互联对象体现了虚拟化的特征。由虚拟化带来了一系列新的问题：无论是计算、网络还是存储都不能靠单独工作来实现更大的能力。一台虚拟服务器能够被创建需要一定的前提，即相对应的存储资源和网络资源要匹配，一台虚拟服务器必须通过统一的管理和调度，把计算所需要的存储和网络资源匹配后才能工作。虚拟服务器在进行复制和迁移时也需要一系列统一管理和协调的动作。集群计算，在虚拟化和自动化之后，新的计算模式可以称为云计算。云计算本身比单个虚拟服务器需要更复杂的网络和存储的联动就绪。从这个角度来讲，在网络上一切行为的开展不再是以设备资源为核心进行管理和调度，而是开始以面向应用和服务的全新方式进行组合。这种转变，要求应用和服务所需的底层架构必须是智能联动的，具备面向应用的自动化配置能力。

另外就是服务质量发生变化。如传统的网络是将标志了地址的“平信”送到目的地，

现在这张网上传递的内容发生了极大的变化,不再是单一的“平信”。如果传递的是金融类信息,就要求绝对的安全和可靠;如果是视频信息,就对实时性、高带宽有很高的要求;如果网络是计算与存储的通道,对服务质量、时延、抖动都有严格要求。Everything over IP,所有接入终端都在对网络传递压力。如果希望网络有高品质的传递,原来网络尽力传递的工作模式就要彻底发生变化,如要把尽力传递网络变成增强型网络,以FCoE为例,必须能够对有严格服务质量要求的业务做无损承载。又如网络必须能够承载多业务,以视频为例,越来越多的视频业务迁移到互联网上,大容量的视频业务承载必须有视频的广播和点播的专业化解决方案。未来网络在技术上能够实现更严格的服务质量保证,从解决方案上网络会走向针对不同业务的多元化专业网络,针对不同的服务质量要求,提供更专业的接入网、城域网、视频网和数据中心互联网络等。

现在网络已经从信息传递角色发展到了更高的角色。之前无论接入什么终端,网络要完成的核心任务都是依照信息发布者的要求传递到目的地。现在网络已经由传输的角色开始向一个应用与终端中间平台的角色迈进,这也是物联网的要求。物联网不是网络有能力把更多的终端接入进来这么简单,本质是当多种终端接入后,如何利用全新的网络平台屏蔽硬件的异构性,协调这些终端工作,服务特定行业的特定应用。基于网络做应用与终端之间的网络中间件,这是给物联网应用做网络就绪的一个很重要的工作。

互联网从未这么快地发展过,在快速发展的过程中面临着巨大的挑战。如果提供的网络满足不了虚拟化、自动化、多业务的高品质承载和物联网络就绪的要求,将无法满足现在和未来的用户需求。现在是自互联网产生以来在基础网络方面前所未有的创新高潮期,相信通过3~5年的努力,整个行业会给最终用户呈现一个全新的网络,它将更强大、更可靠,能更好地改善人们的工作和生活。它,就是新一代网络。

谨以此书与网络从业者共勉,希望这本书能够对相关人员的实际工作有所帮助。在本书成书出版的过程中,大量创新技术及方案仍在不停涌现,由于时间原因不能及时纳入,请各位读者谅解。

· 目 录 ·

第一篇 数据中心

第1章	云计算.....	3
1.1	为什么需要云计算.....	4
1.2	云计算模型.....	6
1.3	云计算的基础架构要求.....	8
1.4	构建与交付云计算.....	9
第2章	新一代数据中心的基础网络架构.....	11
2.1	新一代数据中心的统一基础网络.....	11
2.2	新一代数据中心网络的特征.....	16
2.3	新一代数据中心网络的高可用架构.....	20
2.4	大规模计算网络.....	27
2.5	超高速交换网络.....	35
2.6	数据中心网络如何应对服务器虚拟化.....	48
2.7	虚拟化服务器网络接入层技术对比.....	52
2.8	不同形态服务器的数据中心网络部署.....	61
第3章	新一代数据中心安全建设思路.....	71
3.1	云计算的安全建设思路.....	71
3.2	企业数据中心的安全设计.....	76
3.3	运营商互联网数据中心的安全设计.....	84
3.4	运营商互联网数据中心的增值安全服务.....	90
3.5	虚拟防火墙技术在数据中心的应用.....	94

第4章	新一代数据中心管理.....	97
第5章	新一代数据中心灾备服务.....	101
第6章	典型数据中心网络设计方案.....	111
6.1	超级计算网络设计方案	111
6.2	应对搜索业务流量模型的数据中心网络解决方案.....	116
第7章	数据中心网络性能测试.....	121
第8章	对数据中心网络的展望.....	127

第二篇 广域网

第1章	广域网络的基础架构.....	131
1.1	广域基础网络架构及演进.....	131
1.2	构建高可用的广域网络.....	135
1.3	“一网双平面”——一种新型广域骨干网络架构.....	141
第2章	广域网的资源化设计.....	149
2.1	广域网流量调度方案发展与应用.....	149
2.2	广域网QoS设计思路.....	158
2.3	分层CAR技术	168
2.4	广域网优化的技术实现和展望.....	172
第3章	广域网专网业务隔离与分支接入.....	177
3.1	IP专网VPN技术方案选型	177
3.2	广域专网的MPLS VPN应用	182
3.3	智能广域网分支.....	189
3.4	新型精品化网点.....	193
第4章	广域网安全.....	199
4.1	广域网安全建设的思路和部署.....	199
4.2	广域网环境下的终端准入控制方案.....	206
第5章	广域网管理.....	213
5.1	广域网管理的构成与建设.....	213
5.2	TR069智能分支管理.....	217

第6章 广域网设计与部署最佳实践.....	225
6.1 金融广域网路由快速收敛最佳实践.....	225
6.2 最佳实践案例分析.....	232

第三篇 城域网

第1章 城域电信级以太网的崛起.....	239
----------------------	-----

第2章 电信级以太网关键技术.....	245
2.1 以太网的运营化改造.....	245
2.2 40G/100G 以太网的标准之路	250
2.3 高速接入：万兆全光以太环网.....	254
2.4 VPLS组网可靠性的简化部署.....	261
2.5 城域网的网络虚拟化.....	265
2.6 运营级以太网OAM	271

第3章 电信级以太网应用方案.....	277
3.1 CE技术融合传统传送网.....	277
3.2 城域VPN融合业务平台	282
3.3 三网融合下的流量分析及承载网络建设.....	287
3.4 电信级以太网在集团客户的最新应用.....	290
3.5 云间专线高速互联.....	295

第4章 电信级以太网的部署实践.....	301
4.1 城域网高可靠性部署.....	301
4.2 IRF2解决以太环网冗余保护问题.....	307
4.3 MAC-in-MAC与VPLS融合部署应用.....	311
4.4 运营级以太网服务质量保证.....	317

第5章 电信级以太网测试方法.....	325
---------------------	-----

第四篇 园区网

第1章 虚拟园区网的发展.....	333
1.1 园区网的演进及虚拟园区网1.0.....	333
1.2 虚拟园区网2.0的优势.....	338

第2章	虚拟园区网的应用方案与部署	345
2.1	虚拟园区网2.0的安全部署	345
2.2	虚拟园区网2.0的网络管理	352
2.3	虚拟园区网2.0时代的移动园区网	354

第3章	虚拟园区网的应用实践	359
3.1	虚拟园区网2.0在政务网中的实践	359
3.2	虚拟园区网2.0在企业网中的实践	367

第4章	园区网的发展趋势	373
-----	----------------	-----

第五篇 无 线

第1章	有线无线一体化	381
-----	---------------	-----

第2章	WLAN主要技术标准与进展	385
-----	---------------------	-----

第3章	WLAN一体化安全	391
-----	-----------------	-----

第4章	WLAN应用方案	399
4.1	无线校园网方案	399
4.2	智能移动医疗方案	405
4.3	无线城市方案	411
4.4	无线语音方案	417
4.5	WLAN与3G的融合方案	424

第5章	WLAN的部署与优化	429
5.1	无线网络部署	429
5.2	无线网络优化	437

第6章	WLAN网络测试	445
-----	----------------	-----

第7章	WLAN的绿色设计	449
-----	-----------------	-----

第六篇 安 全

第1章	企业信息系统安全建设的整体思路.....	457
第2章	网络安全.....	463
2.1	安全产品高端化趋势.....	463
2.2	网络与安全的共同融合.....	467
第3章	应用安全.....	471
3.1	基于深度包检测的应用识别原理和实现.....	471
3.2	基于Web应用的漏洞分析及防御实现	476
第4章	终端安全.....	481
4.1	终端安全控制技术的类型.....	481
4.2	网络准入控制的原理和实现过程.....	483
4.3	终端准入实施中常用的身份认证方案.....	485
第5章	统一安全管理.....	489
第6章	法规遵从和等级保护.....	493

第七篇 管 理

第1章	IT管理的发展.....	501
第2章	架构融合趋势下的 IT管理新价值.....	505
第3章	IT从“道路管理”步入“交通管理”.....	509
第4章	构建开放的IT管理系统	513

第八篇 热 点

第1章	IRF.....	521
1.1	网络虚拟化IRF2技术架构.....	521
1.2	基于IRF2的网络安全设计.....	530
1.3	数据中心IRF2架构设计与应用.....	536
1.4	企业园区IRF2架构设计与应用.....	545

1.5	IRF2的部署.....	551
1.6	IRF2对现网的升级及与第三方设备的标准化对接.....	556
1.7	IRF2的高可靠性测试.....	561
第2章	IPv6.....	567
2.1	软件平台对IPv6的支持	567
2.2	IPv6的接入层安全技术	571
2.3	IPv6中的可控组播技术	577
2.4	OSPFv3协议的特点及部署	581
2.5	IPv6协议一致性测试	585
2.6	数据中心的IPv6技术部署	590
2.7	园区网的IPv6技术部署	593
2.8	电子政务外网的IPv6技术部署	600
第3章	可靠性.....	607
3.1	网络产品硬件的可靠性保证.....	607
3.2	网络解决方案的可靠性设计.....	610
3.3	硬件的可靠性测试设计.....	616
3.4	软件的可靠性测试设计.....	618
3.5	网络系统方案的可靠性测试设计.....	624
第4章	绿色.....	629
4.1	绿色IT观——企业社会责任与客户价值实现并重.....	629
4.2	网络产品绿色评估方法.....	632
4.3	绿色企业网解决方案.....	635
4.4	欧盟四大环保指令法规.....	638
	全书缩略语.....	643

第一篇 数据中心

数据中心是当前大中型企业IT建设的重点和热点，随着数据中心建设的深化和优化，IT系统之间的孤立性不复存在，基于数据中心应用的业务创新成为新数据中心时代的主要内容。

新业务的不断出现，应用系统之间复杂的通信关系已经超越了传统IT的分离孤立式架构的约束，要求应用技术架构能够满足面向服务（SOA）的需求；数据中心基础网络架构，不仅作为数据的存储、交换、处理平台，并将为新一代应用架构提供更广阔的业务整合和业务扩展功能。

新的需求也要求网络能够提供灵活的应用扩展能力和一致的业务延续性，层次化网络结构将向着集约化架构发展，将层次化网络扁平化，将复杂的网络模型简化，使数据中心得以脱离物理连接束缚和空间限制等因素，成为企业新业务创新与开发的后台。

因此，新一代数据中心技术着力于高可靠、虚拟（IRF）、100G平台、安全集成及这些综合技术的最佳实践，来实现数据中心的新发展需求。

基于100G平台的端到端IRF数据中心网络架构，有效整合了数据中心传统的分区差异性要求，将复杂的网络结构进行了简化，消除了环路并精简了路由器结构，也将复杂的应用系统交互通路进行了简化，使得应用的数据流路径在网络上确定并可控，保证毫秒级的快速收敛性，并通过高性能集成的安全系统实施有效的安全策略和深度防护，以实现面向虚拟化应用、企业创新业务的伸缩性数据中心交换和集成平台。

新一代数据中心网络平台既可兼容传统业务模式，又能面向全新的业务模型（如云计算等），支持数据中心应用不断演进，并在方案部署实践中覆盖承载、安全、容灾和虚拟化等全面设计。

第1章 云计算

目前，云计算没有统一的定义，这与云计算本身的特征有关。维基百科对云计算的定义是：云计算是一种基于互联网的新计算方式，通过互联网上异构、自治的服务为个人和企业提供按需即取的计算。由于资源是在互联网上，而互联网通常以云状图案来表示，因此以云来类比这种计算服务，同时云也是对底层基础设施的一种抽象概念。云计算的资源是动态扩展且虚拟化的，通过互联网提供，终端用户不需要了解云中基础设施的细节，不必具有专业的云技术知识，也无需直接进行控制，只关注自身真正需要什么样的资源及如何通过网络来获得相应的服务。

当前关于云计算描述的共同特征是：云是一种服务，类似水电一样，按需使用、灵活付费，使用者只关注服务本身。云计算是一种新的IT服务模式，支持大规模计算资源的虚拟化，提供按需计算、动态部署、灵活扩展能力。

图1.1给出了一个用户使用云计算的示意图，用户对云资源的使用不用关注具体技术实现细节，只需关注业务的体验。如当前被广泛使用的搜狗拼音输入法，其实就是一种云服务：搜狗输入法能够以快速简单的方式为用户提供需要的语境和备选的字素，使得文字的编排可以成为激发灵感的一个辅助工具；但是用户并不关注搜狗输入法在后台运行的数千台服务器提供的大型集群计算，这些工作都交给了ISP。



图1.1 云计算视图

1.1 为什么需要云计算

企业的IT建设过程，以当前的基准来衡量，主要有三个阶段，如图1.2所示。

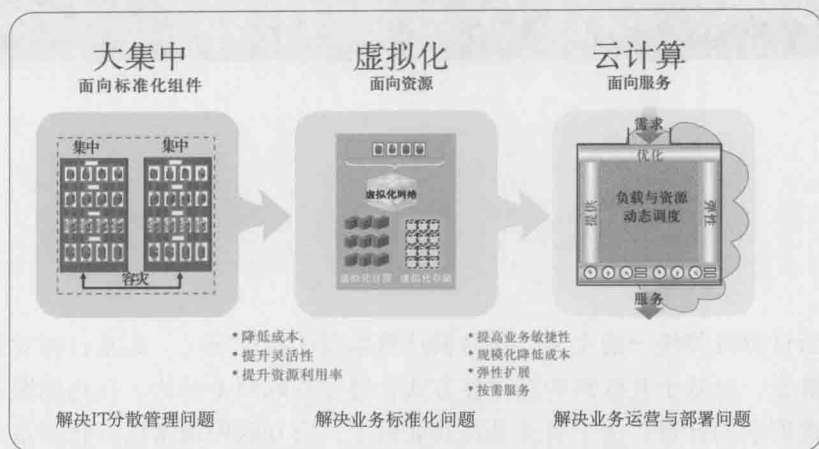


图1.2 企业IT向云计算演进路线图

第一个阶段：大集中阶段

这一过程将企业分散的数据资源和IT资源进行了物理集中，形成了规模化的数据中心基础设施。在数据集中过程中，不断实施数据和业务的整合，大多数企业的数据中心基本完成了自身的标准化，使得既有业务的扩展和新业务的部署能够规划和可控，并以企业标准进行IT业务的实施，解决了数据业务分散时期混乱无序的问题。

在这一阶段中，很多企业在数据集中后期也开始了容灾建设，特别是在2008年雪灾、大地震之后，企业的容灾中心建设普遍受到重视，以金融为热点行业几乎开展了全行业的容灾建设热潮，金融行业大部分的容灾建设的级别都非常高，面向应用级容灾（数据零丢失为目标）。

总的来说，第一阶段过程解决了企业IT分散管理和容灾的问题。

第二个阶段：虚拟化阶段

在数据集中与容灾实现之后，随着企业的快速发展，数据中心IT基础设施扩张很快，但系统建设成本高、周期长，即使是标准化的业务模块建设（哪怕是系统的复制性建设），软硬件采购成本和调试运行成本与业务实现周期并没有显著下降。标准化并没有给系统带来灵活性，集中的大规模IT基础设施出现了大量系统利用率不足的问题，不同的系统运行在独占的硬件资源中效率低下，而数据中心的能耗和空间问题逐步突显出来。因此，以降低成本，提升IT运行灵活性，提升资源利用率为目的的虚拟化开始在数据中心进行部署。

虚拟化屏蔽了不同物理设备的异构性，将基于标准化接口的物理资源虚拟化成逻辑上完全标准化和一致化的逻辑计算资源（虚拟机）和逻辑存储空间。虚拟化可以将多台物理服务器整合成单台，每台服务器上运行多种应用的虚拟机，实现物理服务器资源利

用率的提升,由于虚拟化环境可以实现计算与存储资源的逻辑化变更,特别是虚拟机的克隆,使得数据中心IT实施的灵活性大幅提升,业务部署周期可由数月缩短到一天以内。虚拟化后,应用以VM为单元部署运行,数据中心服务器数量可大大减少,且计算能效提升,使得数据中心的能耗与空间问题得到控制。

总的来说,第二阶段过程提升了企业IT架构的灵活性,数据中心资源利用率得到有效提高,运行成本降低。

第三个阶段:云计算阶段

对企业而言,数据中心的各种系统(包括软硬件与基础设施)是一大笔资源投入。新系统(特别是硬件)在建成后一般经历3~5年即面临逐步老化与更换的问题,而软件技术则不断面临升级的压力。另一方面,IT的投入难以与业务需求匹配,即使虚拟化后,也难以解决不断增加的业务对资源的变化需求,在一定时期内扩展性总是有所限制的。

于是企业IT产生新的期望:IT资源能够弹性扩展,按需服务,将服务作为IT的核心,提升业务敏捷性,进一步降低成本。因此,面向服务的IT需求开始演化到云计算架构上。云计算架构可以由企业自己构建,也可采用第三方云设施,但基本趋势是企业将逐步采取租用IT资源的方式来实现业务需要,如同水力和电力资源一样,计算、存储、网络将成为企业IT运行的一种被使用的资源,无需自己建设,可按需获得。

从企业角度,云计算解决了IT资源的动态需求和最终成本问题,使得IT部门可以专注于服务的提供和业务运营。

这三个阶段中,大集中与容灾是面向数据中心物理组件和业务模块,虚拟化是面向数据中心的计算与存储资源,云计算最终面向IT服务。这样一个演进过程,表现出IT运营模式的逐步改变,而云计算则最终根本改变了传统IT的服务结构,它剥离了IT系统中与企业核心业务无关的因素(如IT基础设施),将IT与核心业务完全融合,使企业IT服务能力与自身业务的变化相适应。

在技术变革不断发生的过程中,网络逐步从基本互联网功能转换到Web服务时代(典型的Web2.0时代),IT也由企业网络互通性转换到提供信息架构全面支撑企业核心业务。技术驱动力也为云计算提供了实现的客观条件,如图1.3所示,在关键领域云计算技术已经就绪。

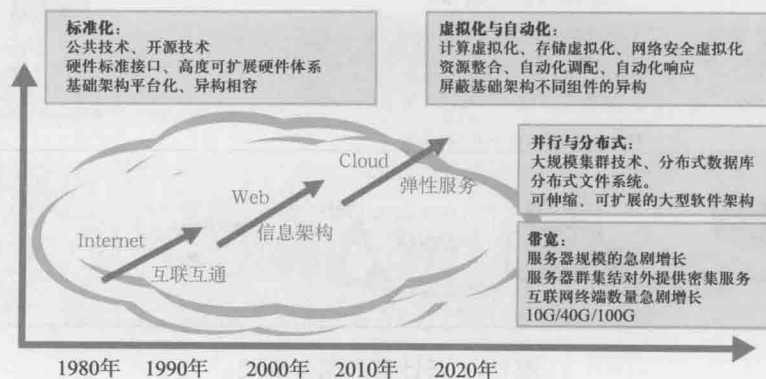


图1.3 云计算的技术基础