

H3C

新一代网络建设 理论与实践

(第2版)

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(第2版)(下册)

杭州华三通信技术有限公司 著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书围绕“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及应对方案。

本书面向IP网络技术领域的相关从业者,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:全2册/杭州华三通信技术有限公司著. — 2版. — 北京:电子工业出版社,2013.3
ISBN 978-7-121-19654-6

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(2013)第035077号

责任编辑:李新社

特约编辑:曲 昕 汪荣萍

印 刷:北京市大天乐投资管理有限公司

装 订:北京市大天乐投资管理有限公司

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:57.75 字数:1452千字

印 次:2013年3月第1次印刷

定 价:268.00元(上、下册)

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zltz@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》。期望本书能够给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

副总裁及首席运营官

· 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。大家习惯了在计算机上输入一个信息，由网络将其送到接收端。很少有人关心当数以亿计的用户连接到庞大的互联网上，网络是如何有效地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，我们必须清醒地意识到技术革新的大幕已经拉开，“新一代网络”也从技术、产品准备和解决方案的角度展现在我们面前。

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，通过Facebook、Twitter形成新的社交关系。当一个具体应用的用户群是以亿计数时，就需要一种全新的计算方式，它把以亿计数的输入信息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。目前超大数据中心的规模已经超过20万台服务器，行业领先的计算集群已经超过5000个节点。当计算规模变得极其庞大时，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、操作系统和数据库，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复制和迁移。虚拟服务器既有比一台物理服务器计算能力小的（1：N），也有成百上千台物理或虚拟服务器集群起来的（N：1）。无论是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：无论计算、网络或存储都不能靠单独工作来实现更大的能力。创建一台虚拟服务器需要一定的前提，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资源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。在虚拟化和自动化之后，集群计算，这种新的计算模式被称为云计算。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。传统的网络是将标记了地址的“平信”送到目的地，而

现在网络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,就对服务质量、时延、抖动都有严格要求。Everything over IP,即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地发生变化,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。未来的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,未来的网络将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。

现在的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将信息传递到目的地。现在的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。物联网不是指网络有能力把更多的终端接入进来这么简单,其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,希望本书能够对相关人员的实际工作有所帮助。《新一代网络建设理论与实践》(第一版)在2011年首次发行后,受到广大读者的喜爱,于是又有了第二版。这一版重点增加了云计算和数据中心章节的内容,此外也对其他各章节进行了增补和修订。在本次成书出版的过程中,仍有大量创新技术在不停涌现,由于时间原因不能及时纳入,请各位读者谅解。

· 目 录 ·

上册

第一篇 云计算和数据中心

第1章	云计算和云就绪网络	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
1.5	云就绪网络的关键技术	10
第2章	新一代数据中心的基础网络架构	17
2.1	新一代数据中心的统一交换架构	17
2.2	新一代数据中心网络的特征	22
2.3	新一代数据中心网络的高可用架构	26
2.4	大规模计算网络	33
2.5	超高速交换网络	41
2.6	数据中心网络如何应对服务器虚拟化	54
2.7	不同形态服务器的数据中心网络部署	58
第3章	新一代数据中心网络设备虚拟化	69
3.1	概述	69
3.2	N:1网络虚拟化IRF技术架构	71
3.3	1:N的网络虚拟化MDC技术架构	79
3.4	VCF纵向虚拟化技术架构	82
3.5	基于IRF的网络安全设计	89
3.6	数据中心IRF架构设计与应用	95

3.7	企业园区IRF架构设计与应用	104
3.8	VCF纵向虚拟化技术在数据中心的应用	110
3.9	IRF的部署	113
3.10	MDC的部署	118
3.11	IRF对现网的升级及与第三方设备的标准化对接	127
3.12	借助IRF技术进行数据中心机房迁移	132
3.13	IRF的高可靠性测试	138
第4章	新一代数据中心虚拟化服务网络接入技术	145
4.1	虚拟计算环境下的网络架构发展进程	145
4.2	vSwitch技术	149
4.3	EVB技术标准	153
4.4	802.1Qbg、802.1BR、VN-Tag的技术比较	161
第5章	新一代数据中心的安全建设	169
5.1	云计算环境下安全问题和防护建议	169
5.2	云计算数据中心网络安全防护部署	174
5.3	企业数据中心的安全设计	180
5.4	运营商互联网数据中心的安全设计	188
5.5	运营商互联网数据中心的增值安全服务	194
5.6	虚拟防火墙技术及其在数据中心的应用	198
第6章	新一代数据中心的管理	201
6.1	云计算环境下的数据中心管理运行	201
6.2	云计算对数据中心管理的要求	206
6.3	数据中心的虚拟化管理	209
6.4	管理自动化:实现基于业务的服务编排	219
6.5	利用CaaS控制虚拟机蔓延	223
第7章	典型数据中心网络设计方案	231
7.1	超级计算网络设计方案	231
7.2	应对搜索业务流量模型的数据中心网络解决方案	236
7.3	高性能数据中心网络的流量收敛设计	240
第8章	数据中心网络性能测试	247
第9章	对数据中心网络的展望	253

第二篇 园区网

第1章 虚拟园区网的发展	257
1.1 园区网的演进及虚拟园区网1.0	257
1.2 虚拟园区网2.0的优势	262
第2章 虚拟园区网的应用方案与部署	269
2.1 虚拟园区网2.0的安全部署	269
2.2 虚拟园区网2.0的网络管理	276
2.3 虚拟园区网2.0时代的移动园区网	278
第3章 虚拟园区网的应用实践	283
3.1 虚拟园区网2.0在政务网中的实践	283
3.2 虚拟园区网2.0在企业网中的实践	291
第4章 园区网的发展趋势	297

第三篇 广域网

第1章 广域网络的基础架构	305
1.1 广域基础网络架构及演进	305
1.2 构建高可用的广域网络	309
1.3 “一网双平面”——一种新型广域骨干网络架构	315
第2章 广域网的资源化设计	323
2.1 广域网流量调度方案发展与应用	323
2.2 广域网QoS设计思路	332
2.3 分层CAR技术	342
2.4 广域网优化的技术实现和展望	346
第3章 广域网专网业务隔离与分支接入	351
3.1 IP专网VPN技术方案选型	351
3.2 广域专网的MPLS VPN应用	356
3.3 智能广域网分支	363
3.4 新型精品化网点	372
第4章 广域网安全	377

4.1	广域网安全建设的思路和部署	377
4.2	广域网环境下的终端准入控制方案	384
第5章	广域网管理	391
5.1	广域网管理的构成与建设	391
5.2	TR069智能分支管理	395
5.3	基于融合的VPN管理方案	401
5.4	QoS管理中的困难与探索	406
第6章	广域网设计与部署最佳实践	413
6.1	金融广域网路由快速收敛最佳实践	413
6.2	最佳实践案例分析	420

下册

第四篇 城域网

第1章	城域网的变革	3
1.1	面向新业务承载的电信级以太网	3
1.2	城域IP骨干网的变革	9
第2章	电信级以太网关键技术	15
2.1	以太网的运营化改造	15
2.2	40G/100G以太网的标准之路	20
2.3	100GE接口的实现及在城域网的部署	24
2.4	高速接入: 万兆全光以太环网	26
2.5	VPLS组网可靠性的简化部署	34
2.6	城域网的网络虚拟化	38
2.7	运营级以太网OAM	44
第3章	电信级以太网应用方案	49
3.1	CE技术融合传统传送网	49
3.2	城域VPN融合业务平台	54
3.3	三网融合下的流量分析及承载网络建设	59
3.4	电信级以太网在集团客户的最新应用	62
3.5	云间专线高速互联	67

3.6 城域网运营级NAT资源池解决方案	71
第4章 电信级以太网的部署实践.....	75
4.1 SR网关热备：传统方式与设备虚拟化技术对比分析	75
4.2 城域网高可靠性部署	81
4.3 IRF2解决以太环网冗余保护问题	86
4.4 MAC-in-MAC与VPLS融合部署应用	91
4.5 运营级以太网服务质量保证	97
第5章 电信级以太网测试方法.....	105

第五篇 无线

第1章 有线无线一体化.....	113
1.1 有线无线一体化的本质与价值	113
1.2 一体化安全	116
1.3 一体化管理	122
第2章 WLAN主要技术.....	129
2.1 WLAN技术标准	129
2.2 智能天线技术	133
2.3 无线控制器的关键备份策略	139
2.4 AC资源池	144
2.5 逐包功率控制	152
2.6 无线管理标准（RFC5833和RFC5834）	155
第3章 WLAN应用方案.....	159
3.1 无线校园网方案	159
3.2 智能移动医疗方案	166
3.3 无线城市方案	173
3.4 无线语音方案	187
3.5 WLAN与3G的融合方案	194
第4章 WLAN的部署与优化.....	201
4.1 构成WLAN网络高品质的主要因素	201
4.2 无线网络部署	206
4.3 无线网络优化	215

4.4	802.11n的实际应用	225
4.5	WLAN抗干扰分析	233
第5章	BYOD	239
5.1	Wi-Fi与BYOD	239
5.2	无感知认证方案技术	245
5.3	BYOD应用中的识别技术	249
5.4	来宾安全准入模式	253
第6章	WLAN网络测试	259
第7章	WLAN的绿色设计	263

第六篇 安全

第1章	企业信息系统安全建设的整体思路	271
第2章	网络安全	277
2.1	安全产品高端化趋势	277
2.2	网络与安全的共同融合	281
2.3	DoS攻击	285
2.4	远程安全接入	289
第3章	应用安全	293
3.1	基于深度包检测的应用识别原理和实现	293
3.2	基于Web应用的漏洞分析及防御实现	297
3.3	跨站脚本攻击	302
3.4	CSRF的攻击与防御	307
3.5	栈溢出漏洞攻击原理及防护技术	311
第4章	终端安全	317
4.1	终端安全控制技术的类型	317
4.2	网络准入控制的原理和实现过程	319
4.3	终端准入实施中常用的身份认证方案	321
第5章	统一安全管理	325

第6章 法规遵从和等级保护	329
---------------	-----

第七篇 管理

第1章 IT管理的发展	337
-------------	-----

第2章 云计算对IT管理的影响	341
-----------------	-----

第3章 架构融合趋势下的IT管理新价值	345
---------------------	-----

第4章 IT从“道路管理”步入“交通管理”	349
-----------------------	-----

第5章 构建开放的IT管理系统	353
-----------------	-----

第6章 Web2.0技术在IT管理系统中的应用	359
-------------------------	-----

6.1 Web2.0技术带来的个性化体验	359
6.2 AJAX局部刷新技术	361
6.3 全新的RESTful Web服务	361

第八篇 IPv6

第1章 IPv6	367
----------	-----

1.1 IPv6主要标准与进展	367
1.2 软件平台对IPv6的支持	369

第2章 IPv6技术	373
------------	-----

2.1 IPv6的接入层安全技术	373
2.2 IPv6中的可控组播技术	379
2.3 IPv6过渡技术	384
2.4 IPv6协议安全及攻击	391
2.5 IPv6网络下的用户管理	395

第3章 IPv6部署	399
------------	-----

3.1 数据中心的IPv6技术部署	399
3.2 园区网的IPv6技术部署	402
3.3 电子政务外网的IPv6技术部署	409

3.4 WLAN网络中的IPv6技术部署	414
----------------------------	-----

第九篇 可靠性

第1章 可靠性	423
1.1 软件系统的可靠性设计	423
1.2 网络产品硬件的可靠性保证	427
1.3 网络解决方案的可靠性设计	430
1.4 硬件的可靠性测试设计	435
1.5 软件的可靠性测试设计	437
1.6 网络系统方案的可靠性测试设计	443

第十篇 绿色

第1章 绿色	449
1.1 绿色IT观——企业社会责任与客户价值实现并重	449
1.2 网络产品绿色评估方法	451
1.3 绿色企业网解决方案	453
1.4 欧盟四大环保指令法规	457
全书缩略语	461

第四篇 城域网

互联网、IT、CT应用正在进行大整合，基于云计算的综合信息服务正成为发展潮流。新的业务形态将极大地冲击现有的IP承载架构，包括IDC、骨干网、城域网等网络。而作为公众服务的主要承载管道，IP城域网正面临两大技术挑战：10倍带宽提速、云业务承载。

挑战一：10倍带宽提速

预计在两年内，城域接入网将面临10倍以上的带宽提速需求。

在家庭宽带领域，每户带宽将从现在的1 ~ 4Mbps升级为20Mbps以上，以支撑高清视频业务。中国电信计划在3年内实现FTTH覆盖，每户带宽20 ~ 100Mbps。

在大客户专线领域，随着云计算及数据集中建设趋势，分支机构到总部的通信量将大幅增长，带宽也将从当前的2Mbps ~ $N \times 2$ Mbps升级到100Mbps级别高速以太专线。据某省运营商统计，20%的集团客户已正式提出带宽升级的申请，另有30%的客户也有提速的需求。

在无线宽带领域，LTE+802.11n的部署使无线单载波速率提升到50 ~ 600Mbps，是当前3G速率的数十倍。

挑战二：云业务承载

传统的IP城域网基本上是为单一的宽带上网业务设计，为满足以云计算为特征的新型业务，需要进行全面的优化改造。

大规模云业务需要端到端高品质网络支撑，包括云内网络、云间网络、云-端网络。云内网络就是DC内部网，云间网络用于连接多个DC，云-端网络用于连接云中心和客户端。城域网涉及的主要是云-端网络和云间网络。

云-端网络需求首先是高带宽，因为企业的数据在向私有云、公有云集中，以前从局域网可以访问的应用现在需要到云中心去访问，因此带宽至少需要提升10倍，并且要求城域网实现较低的网络收敛。其次云-端网络对网络的可靠性、QoS也提出更高的要求，以前尽力而为的城域网模型将严重影响云服务质量。

云间网络需要更高的带宽，如 $N \times 10$ GE专线（大型公有云）、 $N \times$ GE专线（中小型私有云）。为满足跨数据中心虚拟机迁移、集群计算的需求，云间网络必须具备骨干级可靠性、低收敛、低时延、大缓存等特征。另外，云间网络还需要引入全新的云

网络技术，如多中心大二层网络、虚拟集群网络等。

在新一轮IP城域网变革中，电信级以太网（CE）成为颠覆性的力量。CE技术可将城域网核心节点带宽提升到 $N \times 100\text{Gbps}$ ，边缘节点带宽提升到 $N \times 10\text{Gbps}$ ，满足大规模100Mbps/1000Mbps高速接入需求。同时，最新的CE方案已经融合了网络虚拟化、云间互联、控制云等众多新技术，将推动城域网向“智能管道”演进。

第1章 城域网的变革

1.1 面向新业务承载的电信级以太网

自1973年以太网诞生以来，在发展的数十年中，虽然出现了多种技术与其竞争，但都无法阻止该技术快速前进的步伐。今天，以太网无处不在已成事实，超过99%的数据流起源和结束于以太网接口，以太网一统网络的趋势更加明显。基于以太网的众多新技术层出不穷，云计算、物联网、移动互联、数据中心网络、40G/100G、虚拟化、802.11n和IP SAN都是业界关注的热点。

以太网技术显然已经超越了其最初的局域网起源，成为一种吸引人的、强健的解决方案。其中最引人瞩目的质的飞跃，便是电信级以太网CE（Carrier Ethernet）的引入。运营商可利用电信级以太网CE超群的效率和灵活性，部署高质量的、创造收入的新宽带服务，同时大大减少CAPEX（Capital Expenditure，投资成本）和OPEX（Operating Expense，运维成本），使最终用户可以享受到种类更多、更灵活和费用更低的服务。

1.1.1 电信级以太网的发展

电信级以太网又称运营商级以太网，最早由城域以太网论坛（MEF，Metro Ethernet Forum）在2005年初提出。MEF的战略旨在开发“电信级”以太网必要的规范，从而打破以太网只能为局部地区服务的一般看法。按照MEF定义，电信级以太网技术主要以网络能够支持的以太网业务类型和业务所能达到的性能为衡量标准，并不专指某种网络技术，主要包括5方面的内容，如图1.1所示。

电信级以太网CE发挥以太网内在的可伸缩性和灵活性，使其可以轻松地支持高质量和高带宽的服务。通过运营商级OAM（操作、管理、维护）、服务质量保证和故障保护支持能力上的技术增强，电信级以太网已经能为大部分的关键应用提供标准化和高性能的服务。截至2010年，已经有750多家厂商和运营商得到了MEF的认证。以太网服务业务收入持续走强，根据Infonetics研究公司的预测，到2014年以太网服务业务的全球收入可以达到400亿美元。Infonetics最新进行的全球服务提供商调查显示，100%的受访者声称会在2010年部署IP/以太网回传网络，65%的服务提供商计划转向单一IP/以太网回传网络。英国电