

# 新互联网体系理论及关键技术

## Theory and Key Technologies of New Generation Internet

中图分类号: TP393 文献标识码: A 文章编号: 1009-6868 (2008) 01-0017-04

**摘要:** 互联网在可信(安全、可靠、可控、可管)等方面存在严重弊端。为解决这些问题,文章研究和探索新一代互联网体系的基础理论,给出了新网络的体系结构模型;创造性地提出新网络体系下的交换路由模型与理论,建立接入标识、广义交换路由标识及其映射理论;提出普适服务体系模型与理论,创建服务标识及其映射理论、连接标识及其映射理论;并对新互联网体系中的接入控制管理、可信路由及服务质量、多流传输、网络监测管理等关键技术进行了研究和探讨。

**关键词:** 新互联网;交换路由;普适服务;网络体系

**Abstract:** The Internet faces serious trust problems such as security, reliability, controllability, and manageability. The basic principle of future Internet is studied and its architecture is proposed. Then, the fundamental theory of switching and routing is presented, including accessing identifier, switching-routing identifier and the mapping mechanism between them. Meanwhile, the theory and mechanism of pervasive services are brought forward, including service identifier and connecting identifier and their mapping theories. At last, some key technologies of new generation Internet are discussed, such as access control, trustworthy route, quality of service, multi-homing and network management.

**Key words:** new generation Internet; switching and routing; pervasive service; network architecture

张宏科/ZHANG Hong-ke

董平/DONG Ping

杨冬/YANG Dong

(北京交通大学 电子信息工程学院下一代互联网研究中心, 北京 100044)  
(Next Generation Internet Research Center,  
College of Electronics and Information  
Engineering, Beijing Jiaotong University, Beijing  
100044, China)

很好地满足当今应用的需求,严重阻碍着信息网络的进一步发展,急需突破性、跨越式地重新构思和设计一种全新的网络体系,以解决现有互联网在可信方面存在的严重弊端。

### 1 网络的可信性研究现状及发展趋势

可信系统的概念最早由J. P. Anderson教授在20世纪70年代初期提出,研究者大多将其应用于表达信息的可用性、完整性和机密性。后来当人们将其应用于表达网络提供的可信服务时,传统互联网暴露了其在网络安全、可靠、可控、可管等诸多方面的问题。

为此,近年来世界各国纷纷展开了这方面的相关研究。早在2002年,日本的NTT公司就制订了名为谐振通信网络体系结构(RENA)的发展计划<sup>[4]</sup>,该计划在实现可管理的服务质量(QoS),高安全性,高可靠性和通用的移动性以及终端用户的友好性方面有一定的改进。但是,作为一个工程性的发展计划,它没有解决互联网面临的广泛移动性、可信性、多业务融合、普适性等众多问题。

2003年,美国自然科学基金委员会启动了著名的“100×100”下一代

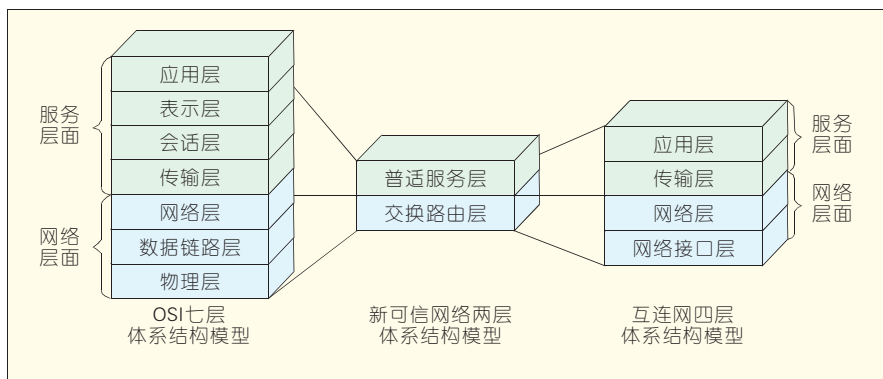
随着科学技术的发展,信息已成为当今推动社会向前发展的巨大动力,信息领域竞争的焦点取决于信息网络技术的掌握和应用水平,而信息网络领域竞争的关键又取决于原创的新信息网络体系及基础理论研究水平。新一代网络将提供普适服务,包括各种话音业务、数据业务、多媒体业务等,因此在新一代信息网络中如何保证网络和服务的可信性,即保证网络中行为和行为结果总是以

预期或可控的形式发生,成为一个非常重要而迫切的课题。

现有互联网的拓扑结构是具有幂律结构的无标度网络<sup>[1]</sup>,导致其对恶意攻击和欺骗的抵御能力十分脆弱;现有互联网路由体系假设所有网络节点处于一个互相信任的环境中,且只提供尽力而为的数据转发服务。由于这些原因,现有互联网出现了大量的安全事件,如地址解析协议(ARP)欺骗、源地址欺骗、域名服务器(DNS)攻击、由路由前缀劫机引起的分布式拒绝服务攻击DDOS攻击<sup>[2]</sup>、垃圾邮件泛滥<sup>[3]</sup>、流量监视<sup>[2]</sup>等,对用户、网络和服务造成严重的损失。

不难看出,现有互联网已经不能

**基金项目:** 国家重点基础研究发展规划项目(“973”计划)(2007CB307101);教育部高等学校科技创新工程重大项目培育资金(706005);高等学校学科创新引智计划(B08002)



▲图1 OSI七层结构及互联网四层结构与新互联网体系结构模型的比较

网络建设项目<sup>[5]</sup>。该项目虽然提出了一种解决因特网面临的部分难题如QoS控制、网络有效管理等的方法,但很难从根本上解决当前信息网络传输多种不同类型业务的普适要求。

2004年,英国电信提出了名为21世纪网络(“21CN”)的下一代网络建设计划<sup>[6]</sup>。该计划从工程的角度为下一代网络的建设提供了很好的借鉴经验,部分解决了诸如多业务、移动性和网络安全等问题,但其仍是对当前网络技术的较大修补与改进。

2005年8月和12月,美国分别提出了著名的全球网络创新环境(GENI)<sup>[7]</sup>和未来互联网网络设计(FIND)<sup>[8]</sup>计划。拟从根本上重新设计新一代网络,以解决现有网络在安全性、移动性、传感性和普适服务支持等方面存在的严重弊端。但其目前还没有形成清晰的理论研究方案。

国际学术界近年来也纷纷撰写论文阐述发展新一代互联网的重要性。英特尔研究中心的Yumerefendi和Chase将可审计性作为新一代互联网设计的核心目标<sup>[9]</sup>,认为新一代互联网的系统行为和状态应该是不可否认和防篡改的。波士顿大学的Mark Crovella和Eric Kolaczky认为新一代互联网应该在负载均衡、错误恢复以及网络管理等几个方面做出较大的改进<sup>[10]</sup>。文献[11-14]则分别从业务拓展、通信方式和质量控制等几个方向对新一代互联网提出了建设的目标。

就中国的发展趋势而言,国家也

非常重视对具有可信性的新一代互联网体系结构、理论及关键技术的研究。在“十一五”计划期间,中国投巨资启动了一系列与之相关的科研工作,如国家“973”计划“一体化可信网络与普适服务体系基础研究”项目,国家“863”计划“新一代高可信网络”重大项目,国家科技支撑计划“可信任互连网”重大项目等。另外,近几年中国学术界也纷纷撰写论文论述这方面的重要性。

总之,从上面的介绍我们不难看出:随着网络技术的不断发展,未来的互联网体系必将发展成为包括支持安全性、移动性、传感性、可靠性、可控性、可管性等特性在内的支持普适服务的新网络体系架构。

## 2 新互联网架构参考模型

### 2.1 新互联网体系结构与模型

通过对传统信息网络分层体系结构理论的长期研究,并对互联网和电信网等机理进行深入剖析,发现各种网络体系结构,都可以划分为两个基本层面:一个是服务层面,一个是网络层面。由此本文创新性地提出一种全新的两层体系结构模型,即“交换路由层”和“普适服务层”,如图1所示。

这种网络体系结构实际上是一个全新的“标识分组网络”(以标识管理;以分组传输),包括“交换路由层”和“普适服务层”两个大的部

分。“交换路由层”的研究目标是在一个可信(安全、可靠、可控、可管)的网络平台上提供多元化的网络和终端接入,保证信息交互的可信性和移动性,并有支持普适服务的能力。“普适服务层”负责各种业务的会话、控制和管理,这些业务包括由运营商或第三方增值服务商提供的各种网络业务,主要是语音、数据、流媒体等,不同的业务用相同的“普适服务层”承载。

### 2.2 交换路由层理论与模型

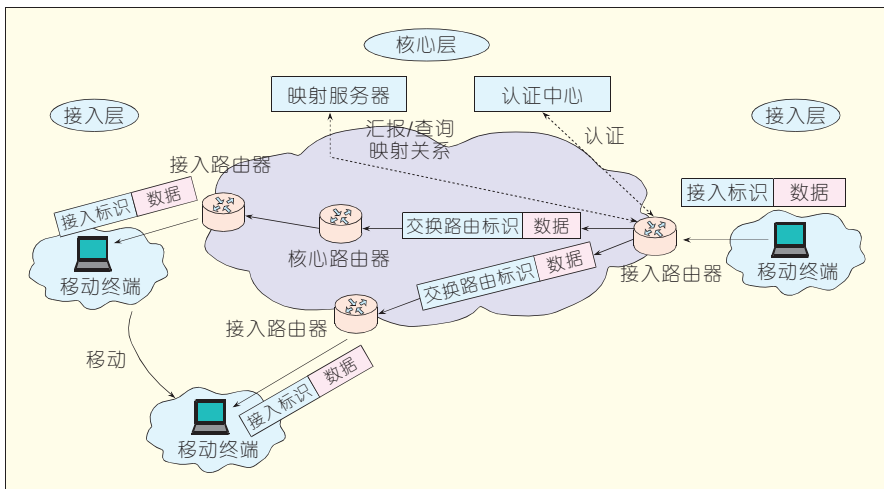
传统IP地址具有语义重载性(IP地址同时表示主机的身份信息和位置信息),导致了一系列难以解决的问题,如IP地址欺骗、传输层无法支持移动性、网络缺乏可控可管能力等。“交换路由层”采用的接入标识与交换路由标识分离映射方法解决了这一问题。

接入标识与交换路由标识分离方法将网络划分为接入层和核心层。网络中有两种标识:接入标识和交换路由标识。接入标识代表了终端的身份信息,只能在接入层使用,而交换路由标识代表了终端的位置信息,只能在核心层使用。“交换路由层”采用“间接通信”模式:在接入层采用接入标识转发数据,而在核心层采用内部的交换路由标识替代接入标识转发;接入层负责各种通信终端的接入,核心层进行控制管理和交换路由,用户的隐私性、网络的安全性、可控可管性和移动性在核心层和接入层中以一种统一的基于标识的方式分别实现。接入标识与交换路由标识分离的网络体系结构如图2所示。

接入标识与交换路由标识分离的网络体系结构具有如下重要作用:

(1)保证用户的隐私性和安全性

接入标识和交换路由标识分离后,代表用户身份的接入标识不会在核心网上传播,使得其他用户不能通过截获核心网的信息分析用户的身份,保证了用户身份的隐私性;也不



▲图2 接入标识与交换路由标识分离映射模型

可能通过用户的身份来截获他们的信息,保证了用户信息的安全性。

#### (2)保证了网络的可控可管性

各种接入网络在申请接入标识时,网络管理者根据用户的签约信息,对各种接入网络进行接入控制和鉴权,鉴权的结果决定是否接受用户连接请求,同时决定为用户提供的服务质量水平。

#### (3)保证了各种接入网络及用户的移动性

各种接入网络在移动到其他位置之后,仅交换路由标识需要发生变化,代表用户身份的接入标识不需要发生变化。这样,用户的连接不需要中断就可以保证用户继续接受各种服务,从而保证了路由变化时保持应用的连续性。

提出了一种基于本体的资源和服务的统一描述机制。具体实现采用了语义网和本体设计的技术,建立了统一的本体描述,其中包括资源的分类和服务的分类,以及对服务和资源的关系进行描述的参数。

#### (2)支持多连接多路径的高效传输协议设计

服务连接的建立是各种网络服务完成必须的过程,高效的连接建立过程是网络设计的重要内容。普适服务层引入“连接标识”的设计,通过将“服务标识”映射到“连接标识”实现服务连接的建立,这种映射的可能形式包括:一对一简单映射、一对多多连接映射、多对一多流映射、多对多复杂映射4种。多连接与多路径

映射模型如图3所示。

### 3 新互联网关键技术研究

现有互联网中的路由协议在设计之初,仅考虑为网络中的节点或应用提供“尽力而为”的路由转发服务,而且路由信息的交互建立在网络节点处于一个相对可信的团体环境这一假定条件之下,而这种假定条件在现有网络中已难以时时成立。新互联网应能阻止和限制一些节点或应用使用网络,或者至少网络中的节点或应用以安全的方式利用网络,并充分利用多流、多路径技术、网络带宽资源管理技术等向其合法用户提供可用并尽可能优的路由,以满足当前用户需求。同时,网络中的不规则事件或行为又能被网络管理人员进行很好地控制和管理。下面将新互联网中涉及的可信方面的关键技术作以简单介绍。

#### 3.1 接入控制管理技术

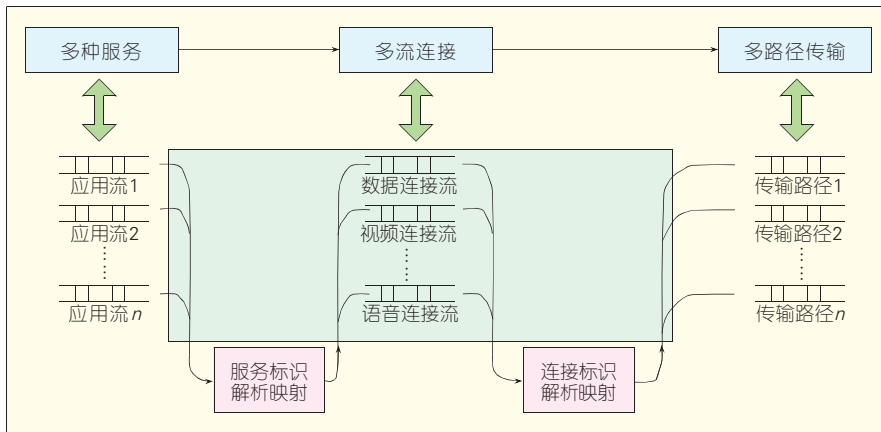
网络接入控制是指对预接入网络的终端进行严格的鉴权管理,保证网络资源和服务只提供给合法注册的用户使用,它是保证网络安全的第一道门槛。但在现有网络中,由于在网络边缘缺乏对终端接入网络进行行之有效的管理,造成大量的非法用户接入事件或者源地址欺骗事件,给网络安全带来重大隐患。而传统网络在接入端将终端的地址、端口等绑定

### 2.3 普适服务层理论与模型

普适服务层主要解决两个问题:网络服务与资源的统一处理;支持多连接多路径的高效传输协议设计。为解决这两个问题,普适服务层分别引入了“服务标识”和“连接标识”。

#### (1)网络服务与资源的统一处理

资源的获取和服务的接入是当前互联网最主要的两种应用,但是在当前的互联网架构之下,资源和服务并没有统一的描述和处理机制。鉴于此,普适服务层通过引入“服务标



▲图3 多连接与多并行路径映射模型



的策略又极大地限制了终端的移动性,不能满足未来互联网对异构网络终端统一接入及终端移动性的需求。因此,在未来互联网体系中,设计一种能够支持异构网络终端统一接入控制的方法是保障未来互联网安全不可或缺的一部分。

### 3.2 可信路由及服务质量

#### (1) 路由安全

传统网络中路由节点建立在相互信任的前提条件之下,一旦这种前提条件被打破,网络中的路由器将无法保证路由的可达性。在未来的互联网中,需要引入安全路由这一概念,即网络中交换路由节点必须以安全的模式通告确知路由,从而保证路由的可达性。

#### (2) 多径路由

在现有网络中运行的路由协议及算法通常只能根据一种规则选取一条到目的路由条目,只是理论上保证路由是连通的。一旦该条链路上的节点失效,路由协议将面临较长的收敛过程。这样就给用户一些实时性较强的应用带来问题。因此未来的互联网除了在尽量减小路由收敛时间上需要改进外,更重要的是网络能够提供冗余路由或者网络能够直接提供多路径传输技术。

#### (3) 服务质量

在可信互联网中我们需要引入服务质量控制过程,以迎合未来网络发展的趋势。首先,未来的互联网一定要满足日益增长的各种各样的多媒体业务的服务质量要求;第二,端到端的服务质量保证是一个研究的重点;第三,新的网络服务质量要体现可控、可管的思想。

### 3.3 多流传输技术

新互联网将全面支持多流,以提高网络的可靠性。现有网络在提供网络服务时,仅建立和维护一条端到端连接的状态信息,无法满足具有不同属性要求的应用需求。新互联网将增

加路径信息侦察和维持功能,为重传路径选择提供动态的参考。

### 3.4 网络监测管理技术

网络的可信性要求系统的行为和结果是可以预期的,能够做到行为状态可监测、行为结果可评估、异常行为可控制。为了达到上述目标,适合未来互联网的网络监测管理技术是必不可少的研究内容。

## 4 结束语

新一代信息网络将逐渐向支持包括安全、可靠、可控、可管等特性在内的新网络体系迈进。在此,本文给出了未来互联网体系结构的一个参考模型,并在交换路由与普适服务两个层面进行了理论阐述和分析。在实现新互联网架构的过程中,诸如接入控制管理、可信路由协议及算法、服务质量保证措施、多流多路径传输、网络监测管理等一系列关键技术,还有待于进一步研究和解决。

## 5 参考文献

- [1] WATTS D J, STROGATZ S H. Collective dynamics of 'small-world' networks [J]. Nature, 1998, 393(4): 440-442.
- [2] NORDSTROM O, DOVROLIS C. Beware of BGP attacks [J]. ACM Computer Communications Review, 2004, 34(2): 1-8.
- [3] RAMACHANDRAN A, FEAMSTER N. Understanding the network-level behavior of spammers [C]// Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '06), Sep 11-15, 2006, Pisa, Italy. New York, NY, USA: ACM, 2006: 291-302.
- [4] NTT. NTT集团将全力以赴,努力实现“中期经营战略”目标[EB/OL]. [http://www.ntt.co.jp/about\\_c/managementstrategy2.html](http://www.ntt.co.jp/about_c/managementstrategy2.html).
- [5] 100 x 100 Project [EB/OL]. <http://100x100network.org>.
- [6] 21CN Project [EB/OL]. [http://www.btglobalservices.com/business/global/news/2005/edition\\_1/21CN.html](http://www.btglobalservices.com/business/global/news/2005/edition_1/21CN.html).
- [7] GENI: global environment for network innovations [EB/OL]. <http://www.geni.net>.
- [8] FIND: future Internet network design [EB/OL]. <http://find.isi.edu>.
- [9] RANGONOTHAN K. Trustworthy pervasive computing: The hard security problems [C]// Proceedings of the 2nd Annual Conference on Pervasive Computing and Communications Workshops, Mar 14-17, 2004, Orlando, FL, USA. Los Alamitos CA, SA: IEEE Computer

Society, 2004: 117-121.

- [10] CROVELLA M, KOLACZYK E. Graph wavelets for spatial traffic analysis [C]// Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 03): Vol3, Mar 30-Apr 3, 2003, San Francisco, CA, USA. Piscataway, NJ, USA: IEEE, 2003: 1848-1857.
- [11] ZHAO B Y, HUANG L, STRIBLING J, et al. Tapestry: A global-scale overlay for rapid service deployment [J]. IEEE Journal on Selected Areas in Communications, 2004, 22(1): 41-53.
- [12] YEOM H, KIM H. An efficient multicast mechanism for data loss prevention [C]// Proceedings of the 7th International Conference on Advanced Communication Technology, Feb 21-23, 2005, Phoenix Park, South Korea. Piscataway, NJ, USA: IEEE, 2005: 497-502.
- [13] GKANTSIDIS C, RODRIGUES P R. Network coding for large scale content distribution [C]// Proceeding of 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 05): Vol4, Mar 13-17, 2005, Miami, FL, USA. Piscataway, NJ, USA: IEEE, 2005: 2235-2245.
- [14] CLARK D, PARTRIDGE C, BRADEN R, et al. Making the world (of communication) a different place [J]. ACM Computer Communication Review. 2005, 35(2): 91-96.

收稿日期: 2007-11-15

## 作者简介



张宏科, 北京交通大学电子与信息工程学院教授, 博士生导师。近年来, 承担多项国家高技术研究发展计划资助项目(“863”计划)、国家自然科学基金项目、国家攻关项目等国家科研项目, 取得了一系列重要的科研成果。目前主要从事下一代信息网络关键理论与技术的研究工作, 作为首席科学家主持国家重点基础研究发展规划项目(“973”计划)“一体化网络与普适服务体系基础研究”的研究工作。



董平, 北京交通大学电子与信息工程学院在读博士研究生。主要研究方向为新一代网络体系结构, 交换路由理论及组播技术。目前作为主要成员参与国家重点基础研究发展规划项目(“973”计划)“一体化可信网络与普适服务体系基础研究”项目的研究。



杨冬, 北京交通大学电子与信息工程学院在读博士研究生。主要研究方向为网络体系结构、路由及网络安全技术。目前作为主要成员参与国家重点基础研究发展规划项目(“973”计划)“一体化网络与普适服务体系基础研究”项目的研究。