

# 可信路由机理及关键技术

## Research on Theory and Key Technologies of Trustworthy Routing

中图分类号: TP393 文献标志码: A 文章编号: 1009-6868 (2009) 06-0013-05

**摘要:** 文章认为由于网络规模的增大以及节点移动、多宿主、网络流量工程等需求的不断增强,使得路由可扩展性、安全性、可靠性等问题凸显。尽管与可信路由相对应的理论技术方案不断提出,但未能从根本上解决网络路由的可信任问题。为此文章提出可信路由体系结构模型、可信域内路由、可信域间路由等新网络环境下的可信路由参考机制,并对可信路由涉及的关键技术,如映射可扩展技术、路由信任机制、多径路由技术、服务质量保证、路由监测管理技术,进行了研究和探讨。

**关键词:** 可信路由; 路由理论; 网络架构; 路由技术

**Abstract:** Due to the increasing network size and the wide use of mobility, multi-homing and traffic engineering, some serious problems such as routing scalability, routing security and routing reliability, arise in the routing system. In spite of many theories and technologies proposed to address the problems, the issues associated with trustworthy routing still could not be solved fundamentally. Therefore, we present a trustworthy routing architecture model, and introduce the reference trustworthy routing mechanisms used in the inner-domain and among inter-domains individually. Meanwhile, several key technologies for trustworthy routing in the new network environment are discussed in this paper, including mapping scalability, routing trust schemes, multipath routing, quality assurance of services, and routing monitoring and management

**Key words:** trustworthy routing; routing theory; network architecture, routing technology

王洪超/WANG Hongchao

郭华明/GUO Huaming

张宏科/ZHANG Hongke

(北京交通大学电子信息工程学院, 北京 100044)

(School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044, China)

美国的GENI<sup>[1]</sup>和FIND<sup>[2]</sup>计划, 欧盟的FIRE<sup>[3]</sup>计划, 中国的国家高技术研究发展计划(“863”)和国家重点基础研究发展规划(“973”)等, 力图建立新的路由体系理论及机制使未来网络充分满足上述需求。

### 1 路由理论相关研究

当前针对路由理论的研究之一首先体现在路由体系结构方面, 着重解决路由规模的可扩展性问题。为此, 互联网结构委员会(IAB)于2006年10月在荷兰举办了首次“路由与地址工作组会议”。会议重点讨论并确定造成互联网路由可扩展性问题的主要因素, 形成了清晰的描述互联网路由可扩展问题的文档, 该文档分析了导致全局路由表的规模快速增长的几个重要原因、阻碍路由器技术快速发展的约束条件以及互联网地址结构中所存在的局限性。该文档已于2007年9月正式成为RFC标准(RFC4984)<sup>[4]</sup>。

目前, 因特网研究任务组IRTF成立了路由研究工作组RRG, 主要进行互联网路由可扩展问题的研究。目前RRG工作组中的提案包括AIRA、APT、CRIO、LISP、IPvLX、IVIP、Six/One、TAMARA和TRRP等<sup>[5]</sup>。纵观这些研究方案, 其主要核心思想都是要将通信

随着科学技术的不断发展, 信息成为推动社会发展的巨大动力, 信息传播的载体——信息网络尤其是互联网已成为人们日常工作和生活不可或缺的通信平台。然而, 随着网络用户数的不断增加, 无论是网络规模还是路由条目数量都经历着前所未有的加速增长, 同时用户的服务需求也呈现出多样化的发展趋势, 传统互联网“尽力而为”转发的设计理念在现实网络环境下暴露出越来越多的缺陷, 很难满足包括路由规模可扩展性、流量工程、路由备份及多

路选择、路由安全性以及网络服务质量保障等方面日益苛刻的需求。

路由体系及理论作为互联网的核心支撑, 在当前网络需求下, 迫切需要得到进一步的扩充和完善。未来的路由机制应该具有新的特性, 使得网络能够适应规模增大而具有良好的可扩展性; 使得网络使用者和运营者有更大的操作空间而具有较好的灵活性; 使得网络能够充分应对各种网络攻击而具有更好安全性; 使得网络能够满足不同业务的需求而具有更好的服务质量保证等, 这些关键点已经为越来越多的科研工作者所认同。为此, 世界各国政府或研究机构都在制订和实施相应的研究计划, 如

**基金项目:** 国家重点基础研究发展规划(“973”计划)课题(2007CB307100)

中节点的身份标志与位置标志相分离,解决传统互联网IP地址语义重载的局限性,只不过对现有网络路由机制的变动程度有所不同而已。但目前RRG工作组中的各种技术方案尚停留在讨论阶段,缺少必要的试验或仿真加以支持。

除此,解决当前互联网路由可扩展问题的提案还有NIRA<sup>[6]</sup>、HLP<sup>[7]</sup>、ROFL<sup>[8]</sup>、AIP<sup>[9]</sup>等。NIRA为主机提供了一种通过不同地址来选择不同路由路径的机制,通过严格的分等级地址分配策略,NIRA可以改善路由的可扩展性问题。HLP是作为BGP的替代协议提出的一种路由协议,同时采用了链路状态和路径向量两种方式,是一种混合式分等级的路由协议,在一定程度上可以解决路由可扩展问题。ROFL是一种完全基于平面标签的新颖路由方式,其有效性和实用性还有待进一步的研究和验证。AIP采用自认证的地址层次结构试图解决网络欺骗以及路由安全等问题,但也仍处于讨论和研究阶段。

对传统路由理论技术的研究,也一直是学术界关注的热点,目前的研究主要体现以下几个方面:

#### (1)路由安全性研究

现有互联网中的路由协议在设计之初,仅考虑到网络目的的一个方面,即为网络中的节点或应用提供路由的可达性信息,而且这种路由可达性信息的交互传送建立在网络节点处于一个互相可信任的团体环境中的假定条件之下,而这种假定条件在现有的网络中已难以时时成立。现有互联网大量路由安全事件的发生,使得人们不得不重新考虑路由机制的安全性。早在2002年,文献[10]就系统指出了域间路由协议BGP存在的安全缺陷。尽管关于提升BGP安全的方案S-BGP<sup>[11]</sup>,soBGP<sup>[12]</sup>等被陆续被提出,但到目前尚未真正实施。

#### (2)路由可靠性研究

现有互联网中的路由协议,对一个给定的前缀只能查找到唯一的一

条“最佳”路径到达目的端。当网络的节点在遭受攻击或者出现链路故障时,现有的路由协议不具备良好的保护机制和快速恢复能力,很难提供稳定可靠的网络服务。在路由可靠性研究方面,文献[13]和文献[14]分别给出了快速重路由和多拓扑路由机制;文献[15]在避让失效节点和链路提供域间路由多样性等方面进行了探索研究;文献[16]则给出可供用户选择的路径多样性方案。这些工作给路由可靠性研究指出了前进的方向。

#### (3)路由可控可管性研究

现有的路由机制对网络中可能出现的诸如个别节点瘫痪导致的路由中断,个别节点或系统的加入引起的路由紊乱,P2P流量肆意占用带宽、各种网络病毒的感染传播和攻击引起的网络资源紧缺等不规则网络行为,很难做到及时探测、快速定位追踪以及及时合理的处理不规则网络行为;此外,网络节点众多,规模庞大,也给网络配置管理带来一定的复杂性。文献[17]对网络中可能存在的域间路由流量劫持的探测技术进行了研究,文献[18]给出了推导企业网络故障定位的方法,文献[19]则建议利用专门信道进行网络路由的管理。尽管如此,有关路由的可控可管性尚未形成行之有效的解决方案,未来路由机制的监管以及高效配置机制尚需完善。

#### (4)路由服务质量研究

现有互联网所提供的是“尽力而为”的转发服务,在这种服务模型下,所有的业务流被“一视同仁”公平地竞争网络资源,业务流传输的可靠性、延迟性等服务质量要求得不到任何保证。对此,IETF先后提出了集成服务<sup>[20]</sup>和区分服务<sup>[21]</sup>两种服务质量体系结构,然而这两种方案在可扩展性和公平性等方面各有不足。多协议标签交换(MPLS)<sup>[22]</sup>将IP路由控制和第二层交换的简单性无缝地集成起来,在不改变用户现有网络的情况下能提供高速、安全、多业务统一的网

络平台。尽管当前MPLS被广泛使用,但其在网络传输效率,网络兼容性,配置复杂性,网络成本以及服务质量颗粒度等方面的不足,还不足以满足当前多种业务的发展要求。

总之,当前网络路由机制在安全、可靠、可控、可管等网络可信问题的研究上,上述提到的各个研究方案主要停留在理论或应用的某个局部目标,他们所作的只是现有网络路由可信任问题的点滴修补,尚没有形成完整的、系统的可充分满足用户和网络需求的路由理论体系,因而也就未能从根本上解决网络路由的可信任问题。

## 2 可信路由内涵

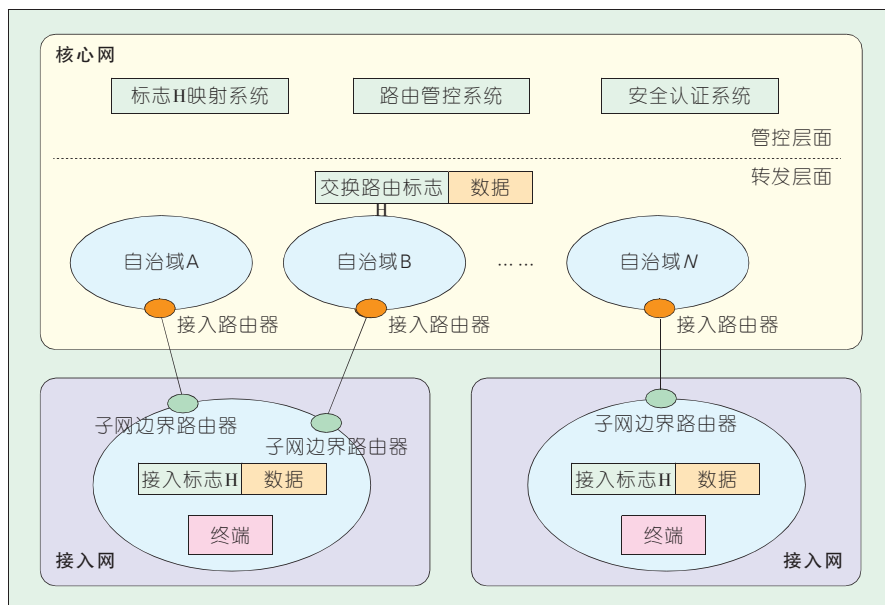
可信系统的概念最早由J.P. Anderson教授在20世纪70年代初期提出,最初只被用于描述信息的可用性、完整性和机密性。后来当其被应用到网络时,传统的路由机制在安全性、可靠性、可控可管等方面暴露了诸多问题。我们说一个系统是可信的,通常是指系统的行为和结果是可预期的。推而广之,可信路由是指网络在任何情况下,都能按照用户及网络运营者的预期为用户提供安全、可靠、可控可管的、满足用户网络服务质量需求的路由。为此,可信路由的设计要求应包含以下几方面:

#### (1)空间隔离保护

应区分接入网和核心网,分别引入不同的标志空间,在核心网和接入网间部署边界路由设备,提供基于标志的映射服务,从而使路由规模的变化独立于用户网络规模的大小,使网络具有更好的可扩展性,同时充分保证核心网络设备的安全。

#### (2)身份与位置分离

应将节点的身份与位置信息分离,建立全网统一的身份与位置映射机制,实现映射信息安全、快捷的在线管理,实现节点位置的隐私性保护以及节点移动情况下的持续连接,从而满足用户越来越强的移动性以及



▲图1 可信路由体系结构参考模型

隐私性需求。

### (3)可信路由寻址

应采用必要的身份鉴别机制以及路由消息的安全传输机制,确保路由节点的身份的真实性,路由可达性信息的保密性、完整性;实现网络路由节点间多路机制,同时应提供路由的备份以及快速恢复能力,从而使网络具有更加安全可靠的服务能力。

### (4)服务质量保证

应采用集中和分布式相结合的方式,充分提取网络资源利用状态,针对不同的业务应用及其服务质量需求,提供满足需求的更高粒度区分的路由。

### (5)网络安全防护

应建立健全全网分布式安全检测防护系统,实现网络传输和网络状态的综合分析,同时提供一定的网络错误诊断能力和行之有效的安全管理机制及策略,使网络路由机制具有更好的可控可管性。

## 3 可信路由参考机制

### 3.1 可信路由体系结构模型

基于以上对可信路由理论技术的研究,本节提出了一种可信路由体

系结构模型,新结构采用不同的网络标志分别代表主机的身份信息和位置信息,并且把原IP网的单一地址空间划分为两个不同的标志空间,两个标志空间内分别采用不同的路由方式,并形成相对独立的路由空间,两个标志(路由)空间之间通过标志映射的方法完成寻址和选路。新网络结构划分为接入网和核心网,包含两种标志:接入标志和交换路由标志。接入标志代表了终端的身份信息,只能在接入网使用,而交换路由标志代表了终端的位置信息,只能在核心层使用。新路由体系结构采用“间接通信”模式连接两个标志空间:在接入网采用接入标志转发数据,而在核心网采用内部的交换路由标志替代接入标志转发;接入网负责各种通信终

端的接入,核心网进行控制管理和交换路由。新可信路由体系结构如图1所示。

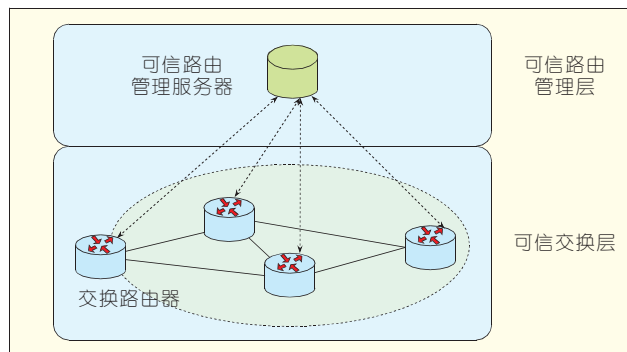
在上述的可信路由体系结构参考模型中,接入网与核心网的分离,使得接入网的动态变化不会出现在的核心网上,保证了核心网的相对稳定;接入网的多家乡、流量工程等也不会引起核心网的路由表的增长和不稳定。代表用户身份的接入标志不会在核心网上传播,使得其他用户不能通过截获核心网的信息分析用户的身份,保证了用户身份的隐私性;也不可能通过用户的身份来截获他们的信息,保证了用户信息的安全性。同时,接入网内的终端无法知道核心网内的网络设施的交换路由标志或是其他终端的交换路由标志;接入网内的终端也就无法针对核心网的网络设施或是某一终端进行攻击,保证了核心网网络设施和数据的安全性。新路由结构仍分为域内路由和域间路由两部分。

### 3.2 可信域内路由

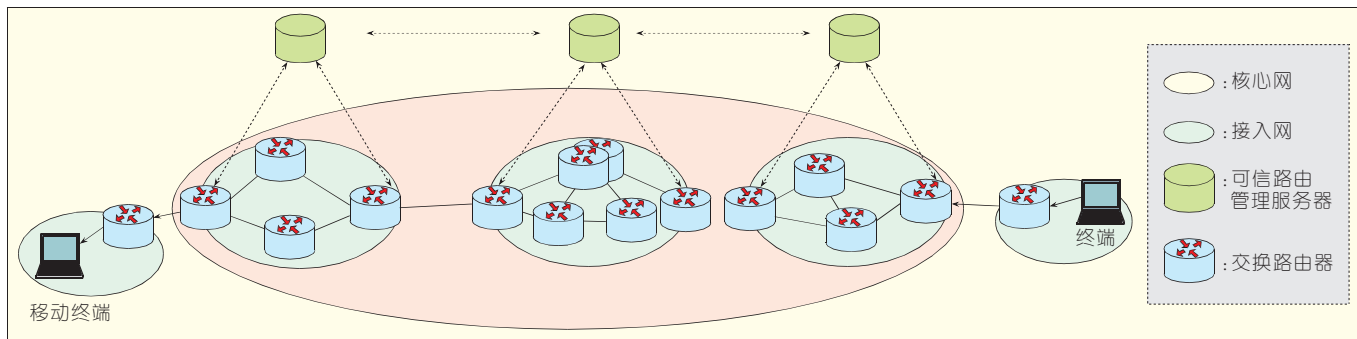
新可信路由体系结构域内路由采用集中式和分布式路由相结合的方式,如图2所示。在每个域内用一个可信路由管理服务器作为集中可信路由管理层;其他基础网络设备组成分布式交换路由层。交换路由层除运行传统的链路状态协议外进行路由转发外,还通过全局流标签的转发的方式进行转发。

可信路由管理服务器和交换路由器组成公钥基础设施(PKI)结构,可

图2  
新可信路由体系结构域内路由结构







▲图3 新可信路由体系结构域间路由结构

信路由管理器作为可信第三方,负责认证域内的交换路由器的认证,并分配公私钥。交换路由器之间通过签名机制对路由通告相互认证。可信路由管理服务同时收集域内的网络状况,为相应的数据流分配全局流标签,同时在相应的交换路由上建立起流标签转发表,使数据流在转发路径上快速转发。这种方式保留了传统单路径路由的路由寻址方式的同时,增加了域内网络资源的统一调度和管理机制,可以为不同的数据流在不同的条件下,建立不同的转发路径,避免网络拥塞,保证服务质量,增加网络的可用性,保证了网络的可控可管性。

### 3.3 可信域间路由

新可信路由体系结构域间路由采用的是基于自认证(Self-certifying)的自治域号的多路径路由方式,如图3所示。因为域间路由更多的是体现了自治域之间的商业竞争关系,无法建立起基于可信第三方的PKI结构,采用基于自认证的自治域号路由就很好的解决地址欺骗的问题。每个域的自治域号为其公钥的Hash值,通过这种命名体系,保证了地址的不可欺骗、抵赖性。再建立起互信后,每对互信自治域之间再建立基于私钥体制的后续通告加密算法,这样可以加快解密的效率。

路由的通告路径时,每个自治域根据策略可通告多条路径,保证每个自治域的独立性和路由的可控制性。通告中包含完整的路径信息,保证了

丰富的路由策略。每个域建立多路径的转发表,发送端通过源路由的方式进行域间选路。发送数据前,发送端的可信路由管理通过可信路由管理层与路径上的其他域内的可信路由管理器协商服务等级、流量等消息。同时,在每个包头加入认证消息,用作去其他域的授权和认证数据包。

## 4 可信路由关键技术研究

## 4.1 映射可扩展技术

接入网与核心网分离以及节点身份与位置分离纵然使得网络路由机制得到良好的可扩展性,但大量接入标志和交换路由标志的映射信息的存储及维护无疑带来了映射系统自身的可扩展性问题。解决好大规模映射信息存储,更新频率以及查询时延等问题,仍是未来可信路由需要研究的关键技术之一。

## 4.2 路由信任机制

解决路由机制的可信问题,首先需要解决路由由节点之间的信任问题。只有参与路由的网络节点彼此信任,才能确保网络节点后续的网络行为以及传送的信息的真实性、可用性。其次,路由消息传输的安全在可信路由机制中,也是不可或缺的组成部分,是保证路由信息可用性的前提。

### 4.3 多径路由技术

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,导致的可靠性差。未来的可信路由要同时提供多条备份路径,并且可以在链路失效和拓扑变化时,进行了快速切换,增加路由的可靠性。研究基于多个下一跳的多径路由技术,对于提高可信路由机制的可靠性非常重要。

#### 4.4 服务质量保证

当前用户服务需求的多样性对网络路由机制提出了更高的粒度需求。新的可信路由机制需要将用户业务的服务质量要求尽量无失真地映射到路由机制中,为用户提供最大限度质量需求保证的路由。研究适用普适服务要求的,能充分满足业务带宽、延迟、抖动和丢包率等服务质量要求的路由机制,对体现路由的可信具有重要意义。

#### 4.5 路由监测管理技术

可信路由机制要求网络行为和结果是可以预期的,保证给用户仅提供满足其业务需求的网络传送服务。因此在可信路由机制下,首先要做到网络状态的可监测性,而且具备对异常网络行为的快速诊断、追踪定位以及自我修复能力,其次,高效的配置管理也是可信路由机制追求的目标。

## 5 结束语

随着网络规模增大, 用户移动,

多宿主,网络流量工程广泛使用以及用户业务需求多样化的发展趋势,传统路由体系理论无法从根本上解决路由的可信任问题,亟待新的可信路由理论体系出现,从而为用户以及网络运营者提供充分满足其需求的可信信任路由。

因此,本文在对当前路由理论研究现状介绍和总结的基础上,给出了未来可信路由机制的内涵,并据此给出了一套适合未来网络需求的可信路由参考机制,最后对可信路由涉及的关键技术进行了研究和探讨。

## 6 参考文献

- [1] GENI: global environment for network innovations [EB/OL]. [2009-08-01]. <http://www.geni.net>.
- [2] FIND: future Internet network design [EB/OL]. [2009-06-19]. <http://find.isi.edu>.
- [3] FIRE: Future Internet research & experimentation [EB/OL]. [2009-07-13]. [http://cordis.europa.eu/fp7/ict/fire/home\\_en.html](http://cordis.europa.eu/fp7/ict/fire/home_en.html).
- [4] MEYER D, ZHANG L, FALL K. Report from the IAB workshop on routing and addressing [R]. IETF RFC 4984, 2007.
- [5] RRG: Routing Research Group [EB/OL]. [2009-07-15]. <http://tools.ietf.org/group/irtf/trac/wiki/RoutingResearchGroup>.
- [6] YANG X, CLARK D, BERGER W. NIRA: A new inter-domain routing architecture [J]. IEEE/ACM Transactions on Networking, 2007, 15(4):775-788.
- [7] SUBRAMANIAN L, CAESAR M, EE C T, et al. HLP: A next generation inter-domain routing protocol [C]//Proceedings of Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM' 05), Aug 22-26, 2005, Philadelphia, PA, USA. New York, NY, USA: ACM, 2005:13-14.
- [8] CAESAR M, CONDIE T, KANNAN J, et al. ROFL: Routing on flat labels [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, 2006:363-374.
- [9] ANDERSEN D G, BALAKRISHNAN H, FEAMSTER N, et al. Accountable Internet Protocol (AIP) [C]// Proceedings of Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM' 08), Aug 17-22, 2008, Seattle, WA, USA. New York, NY, USA:ACM, 2008: 339-350.
- [10] MURPHY S. BGP security vulnerabilities analysis [R]. IETF RFC 4272, 2006.
- [11] KENT S, LYNN C, SEO K. Secure border gateway protocol (S-BGP) [J]. IEEE Journal on Selected Areas in Communications, 2000, 18(4):582-592.
- [12] WHITE R. Securing BGP through secure origin BGP [J]. The Internet Protocol Journal, 2003, 6(3):15-22.
- [13] SHAND M, BRYANT S. IP fast-reroute framework [EB/OL]. [2009-06-10]. <http://tools.ietf.org/html/draft-ietf-rtgwg-ipfrr-framework-06>.
- [14] KYALBEIN A, HANSEN A F, CICIC T, et al. Fast IP network recovery using multiple Routing Configurations [C]// Proceedings of 25th IEEE International Conference on Computer Communications (INFOCOM' 06), Apr 23-29, 2006, Barcelona, Spain. Piscataway, NJ, USA:IEEE, 2006:01-11.
- [15] XU Wen, REXFORD J. MIRO: Multi-path Interdomain Routing [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, 2006:171-182.
- [16] YANG Xiaowei, WETHERALL D. Source selectable path diversity via routing deflections [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, 2006:159-170.
- [17] BALLANI H, FRANCIS P, ZHANG Xinyang. A study of prefix hijacking and interception in the Internet [C]// Proceedings of Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM'07), Aug 27-31, 2007, Kyoto, Japan. New York, NY, USA:ACM, 2007:265-276.
- [18] BAHL P, CHANDRA R, GREENBERG A, et al. Towards highly reliable enterprise network services via inference of multi-level dependencies [C]// Proceedings of Conference on Applications, Technologies, Architectures, and Protocols for Computer

- Communications (SIGCOMM' 07), Aug 27-31, 2007, Kyoto, Japan. New York, NY, USA:ACM, 2007:13-14.
- [19] BALLANI H, FRANCIS P. CONMAN: A step towards network manageability [C]// Proceedings of Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM' 07), Aug 27-31, 2007, Kyoto, Japan. New York, NY, USA:ACM, 2007:205-216.
- [20] BRADEN R, CLARK D, SHENKER S. Integrated services in the Internet architecture: An overview [R]. IETF RFC1633, 1994.
- [21] BLAKE S, BLACK D, CARLSON M, et al. An architecture for differentiated services [R]. IETF RFC2475, 1998.
- [22] ROSEN E, VISWANATHAN A, CALLON R. Multiprotocol label switching architecture [R]. IETF RFC3031, 2001.

收稿日期:2009-08-06

## 作者简介



王洪超, 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。



郭华明, 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路由、网络体系结构、网络处理器。



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, 主要从事下一代信息网络关键理论与技术的研究工作。

## 李克强赞中兴通讯与澳电是两国高新技术合作领头羊

【本刊讯】2009年11月3日, 澳大利亚悉尼, 国务院副总理李克强及其率领的中国代表团主要成员在澳大利亚电信总裁David Thodey和中兴通讯总裁殷一民的陪同下, 参观了澳大利亚电信悉尼总部。李克强指出: “中兴通讯和澳大利亚电信是中澳两国高新技术领域合作的

‘领头羊’, 希望中兴通讯和澳大利亚电信在今后的合作中取得更大的成绩!” 近年来, 中兴通讯与澳大利亚电信在澳洲本地和全球市场的合作广泛而深入, 其中, 尤以样板项目——香港CSL网络最为外界瞩目。终端方面, 通过对澳洲用户的贴身定制, 目前, 澳大利亚平均每8人中就有1人使用中兴通讯的3G终端产品。