新一代互联网关键技术

苏金树　刘宇靖　著

科学出版社

新一代互联网关键技术

苏金树　刘宇靖　著

科学出版社
北京

内 容 简 介

为探索新一代互联网如何更好地适应人工智能、云计算、大数据、移动互联网等领域的发展需求，本书阐述新一代互联网部分关键技术，既包括整体的网络体系结构，也包括各组成部分的核心技术，同时涵盖国内外主要研究项目。本书的研究成果得到国家973计划、863计划、国家自然科学基金项目和国防科学技术研究项目等的支持。希望能够对新一代互联网的发展起到积极的促进作用。

本书可供从事网络技术研究的科研人员、工程技术人员、高等院校相关专业的师生参考。

图书在版编目(CIP)数据

新一代互联网关键技术/苏金树，刘宇靖著. —北京：科学出版社，2019.11
ISBN 978-7-03-060378-4

Ⅰ.①新… Ⅱ.①苏… ②刘… Ⅲ.①计算机网络 Ⅳ.①TP393

中国版本图书馆CIP数据核字(2019)第006144号

责任编辑：张艳芬 / 责任校对：郭瑞芝
责任印制：吴兆东 / 封面设计：蓝 正

科学出版社出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com

北京盛通商印快线网络科技有限公司 印刷

科学出版社发行 各地新华书店经销
*
2019年11月第 一 版 开本：720×1000 1/16
2020年 1 月第二次印刷 印张：15 1/4
字数：365 000

定价：139.00元

（如有印装质量问题，我社负责调换）

前　言

2019年是互联网诞生50周年。互联网为人类社会发展做出了巨大贡献，被誉为20世纪最伟大的工程成就。自诞生至今，互联网已发展成为现代社会不可或缺的一部分，科技、教育、政务、社会、生活，乃至国家基础设施都高度依赖互联网。互联网直接推进了云计算、大数据、物联网和人工智能的发展，也直接推进了网络空间这个新领域的诞生。

在互联网应用领域越来越广泛的同时，随着应用需求的不断变化，新一代互联网技术如何更好地适应人工智能、云计算、大数据、移动互联网等领域的发展需求，是学术界和工业界不断探索的新问题。互联网自身也面临着诸多问题和挑战，需要不断完善。新一代互联网面临的问题归纳起来主要包括三方面：①网络体系结构内在缺陷带来的脆弱性；②互联网的复杂性日益提高，导致网络可管性差、可控性差；③现有网络的生存性设计难以满足关键应用的需求。

学术界和工业界探索了20多年，将互联网分为如下三个阶段：

第一阶段是1996年美国政府发起的NGI(Next Generation Internet)计划和美国100多所大学联合推动的Internet2。该阶段在互联网组播和服务质量保证等方面做出了诸多卓有成效的研究。

第二阶段是美国国家科学基金会于2005年先后启动的FIND(Future Internet Design)计划和全球网络创新环境(Global Environment for Networking Innovations，GENI)计划。FIND计划的愿景是研究未来15年核心骨干网络体系结构、未来15年边缘网络体系结构、未来15年网络体系结构对用户需求的支持。GENI计划的愿景是研究满足21世纪需求的下一代网络体系结构的计划。欧洲也于2007年启动了FIRE(Future Internet Research and Experimentation)计划。这些计划均提出摆脱当前互联网体系结构的束缚，对网络体系结构进行重新设计，以满足未来互联网发展的需求。

第三阶段是美国国家科学基金会支持的五个项目：XIA(expressive Internet Architecture)项目主要研究面向安全的网络体系结构；MobilityFirst项目主要研究面向移动的网络体系结构，并考虑与5G的融合；Nebula项目则是面向云计算的网络体系结构；NDN(Named Data Networking)项目希望研究面向内容分发的网络体系结构；ChoiceNet项目则是面向经济模型选择的网络体系结构。

学术界在研究过程中达成了一些共识，例如，需要支持位置和身份分离，需要支持可追溯性，需要支持多宿主和多路径，需要实现控制和数据分离，需要实现网

络快速自愈恢复，需要支持网络的内在移动性；但是也存在诸多分歧，例如，网络应该简单还是智能？控制应该分布还是集中？协议实现应该采用协议栈还是协议堆？等等。

本书内容源自作者20多年来在新一代互联网领域的研究成果。

全书共6章。第1章介绍新一代互联网研究概况，由当前互联网技术面临的问题入手，归纳总结新一代互联网体系结构研究过程中的共识与分歧，同时提出一种新型的网络体系结构。第2章介绍新一代互联网研究重要计划，给出国际上的主要研究计划与主要研究项目。第3章～第6章重点讨论新一代互联网的部分核心技术。第3章介绍多路径路由技术，综述在多样性、可靠性、安全性需求的牵引下涌现出的各种域间多路径路由协议，并提出一种新的区域化域间多路径路由协议。第4章介绍域间路由安全技术，包括互联网重大事件的域间路由变化特性分析、前缀劫持对路由系统的影响分析及检测方法，以及级联故障对域间路由系统生存性的影响分析。第5章介绍TCP加速技术，针对新一代互联网TCP处理面临的问题，提出路由器辅助的拥塞控制机制与TCP硬件加速技术。第6章介绍互联网流量工程与优化方法，在综述当前网络流量工程研究进展的基础上，提出一种新的混合多优化目标的算法。

在撰写书稿过程中，戴斌、王圣、孟兆炜给予了很大的帮助，赵锋、王小峰、曾迎之、曹继军、戴艺等在准备书稿过程中提供了大量素材，在此一并表示感谢。

限于作者水平和学识，书中难免存在不足之处，敬请读者批评指正。

目　录

第1章　新一代互联网问题与挑战

互联网为人类社会发展做出了巨大贡献，被誉为20世纪最伟大的工程成就，也直接推进网络空间(cyberspace)的诞生和发展。

为满足人类向往美好生活的不断增长的需求，互联网技术作为云计算、大数据、人工智能等领域的基础技术，特别是高性能网络技术作为互联网核心技术，面临着诸多问题和挑战。

为此，学术界和工业界已经探索十多年。例如，从20世纪末开始，美国启动了下一代倡议(Next Generation Initiative，NGI)计划，100多所大学联盟构建的互联网2(Internet2)、2005年美国国家科学基金会(National Science Foundation，NSF)先后启动了未来互联网设计(Future Internet Design，FIND)计划、全球网络创新环境(Global Environment for Networking Innovations，GENI)计划。欧洲也于2007年启动了未来互联网研究与实验(Future Internet Research and Experimentation，FIRE)计划。这些计划均提出摆脱当前互联网体系结构的束缚，对网络体系结构进行重新设计，以满足未来互联网发展的需求。

FIND计划研究方向包括：未来15年核心骨干网络体系结构、未来15年边缘网络体系结构、未来15年网络体系结构对用户需求的支持。FIND侧重于未来互联网体系框架的研究，直接支撑着GENI行动计划的实施。

GENI计划希望研究满足21世纪需求的下一代网络体系结构。GENI计划认为，目前互联网安全脆弱性主要源自当初互联网体系结构和协议设计假定网络运行在一个良性、可信的环境中，几乎没有考虑网络的安全问题。网络体系结构固有的脆弱性是当前网络安全问题的根本来源。为此，GENI计划试图从底层开始对互联网体系结构进行重新设计，并把安全性和鲁棒性作为设计的基本要求。传统的网络安全研究集中在数据泄漏和数据损坏的防范上。GENI计划认为，还应当增强对攻击和失效情况下网络的可用性和恢复能力的研究。未来互联网应该具有很强的生存能力，应能在面对国家危机时提供服务。为了提高网络的安全性和鲁棒性，应当加强网络管理，包括网络配置、系统升级、状态管理、故障诊断及监测修复等。

FIRE计划是欧盟启动的一项长期研究计划，启动资金为4000万欧元。人们期望FIRE计划的目标是促进网络新思想的发展，通过自下而上的开放式研究解决当前互联网面临的安全性等方面的问题。

GENI计划和FIRE计划都特别强调实验驱动性研究的重要性，GENI计划和

FIRE 计划的重要任务之一就是构建方便、真实的实验环境，以支持新型体系结构及相关技术的研究。

美国国防部认为，当前的互联网技术不足以作为可保障全球网络(assurable global networks，AGN)的基础并且当前网络的脆弱性是由高级研究计划署网络(Advanced Research Projects Agency Network，ARPANET)设计原则的优先顺序不同导致的。在 ARPANET 设计原则中，首要的是互联，最末位的是可追溯。假设将可保障性作为首要设计原则，那么很可能出现非常不同的设计。因此，美国国防高级研究计划局(Defense Advanced Research Projects Agency，DARPA)的战略技术办公室(Strategic Technology Office，STO)于 2006 年 12 月中旬发布征求意见书，征求能给 AGN 奠定基础的研究思想和方法，并于 2007 年 2 月召开了战略研讨会。会议收到了来自美国电话电报(American Telephone & Telegraph，AT&T)公司、国际商业机器公司(International Business Machines Corporation，IBM)、英特尔公司(Intel Corporation，简称 Intel)、波音幽灵工厂、BAE 系统公司、加州大学、佐治亚理工学院、普林斯顿大学等知名企业、学校的响应。

本章将概要归纳这些计划面临的问题、对应的研究方法，以及取得的共识与面临的分歧。

1.1 面临的三类问题

互联网技术在安全性及生存性方面存在的问题可以归纳为以下三类。

1. 体系结构内在的缺陷带来脆弱性

早期互联网设计理念主要强调开放性和共享性，安全保障则放在相对次要的位置。无论是网络体系还是协议体系，都没有考虑安全性问题，这导致互联网面临诸多问题，如垃圾邮件、分布式拒绝服务攻击等，网络内在机理与特性决定了互联网技术的内在脆弱性。体系结构内在主要缺陷涉及以下四方面。

1) 隔离方面

在协议体系上，控制平面和转发平面缺乏有效隔离。当前网络的控制平面和转发平面虽然在功能上进行了一定的逻辑区分，但是两个平面的数据混合在同一传输信道，没有对其传输优先级进行划分。这会引发两方面的严重后果。一方面，控制平面很容易受到来自转发平面信息的影响，用户可以很容易地通过转发平面进入控制平面；另一方面，针对转发平面的攻击很容易影响控制平面的可用性，如果网络的转发平面受到拒绝服务攻击，那么很容易导致控制平面也不可用。

2) 设计方面

在协议实现上，软件设计存在缺陷。当前网络的大量攻击都是由软件设计缺

陷引起的，任何微小的软件缺陷都可能导致致命的漏洞。软件的复杂性经常导致测试的不完整性，很多漏洞难以发现。恶意网络用户可以利用这些缺陷发起攻击，例如利用缓冲区溢出来攻击协议漏洞。尤为严重的是，很多网络软件或设备都是成体系地部署在网络中，加之应用环境的复杂性，导致系统级测试难以有效开展，因此一旦利用软件漏洞攻破单点，就会形成长驱直入、迅速传播的后果。

3）协同方面

在安全体系上，安全部件缺乏自主协同机制。当前网络部署了很多安全部件，这些安全部件是相互独立的，它们只能为某一系统或者某一系统的部分提供某种特定的安全防护。即使有些联动，联动也主要是单点上多个安全部件的配合，根本谈不上安全部件之间全局性、一体化的协同防御。网络各种安全防护、安全检测和安全响应部件没有共享安全信息，安全部件也缺乏与网络设备、用户终端和管理员之间的协同，这导致整个网络的安全防护效能低下，难以做到及时准确地进行整体防御，无法保证网络各端点的安全性和可控性。针对某个局域网络发起的攻击，可以很容易地快速扩散到整个广域网，例如，在局域网 A 中扩散的蠕虫病毒，即使已被正确识别，由于缺乏协同机制，也不能被局域网 B 感知，从而使 B 有效地控制病毒扩散。体系安全的缺乏，很容易导致安全策略上的冲突，安全策略的不一致可能会产生更为严重的安全后果，分散的安全部件还不利于安全事件的搜集、整理、分析，也不能提前预防和及时控制安全风险。

4）追踪方面

在安全实现上，无法有效追踪攻击者的身份。在当前网络中，身份是应用层的概念而非网络层的概念。网络层缺乏对节点身份的支持，网络协议往往将网络地址作为网络节点的唯一标识。许多网络服务都基于网络地址对用户进行认证和授权，但是在传统互联网体系中，攻击者可以很容易假冒网络地址。另外，当前网络缺乏对报文中源网络地址真实性的鉴定机制，由于边缘路由器在转发报文时不提供对源地址有效性的检查，因此攻击者的身份难以有效追踪。

2. 复杂性日益提高导致网络可管性差

1）管理深度方面

在管理深度上，智能化管理需要网络单元广泛内嵌管理元素。为了适应不断扩大的互联网规模和不断出现的新型应用，互联网基础设施也不断地复杂化，主要体现在网络规模扩大导致的域间路由系统复杂化、无线设备随时随地接入带来的网络边缘复杂化，以及为满足各种安全目标而部署各种透明中间设备[如防火墙、网络地址转换(network address translation，NAT)网关等]带来的分组处理流程的复杂化。然而，TCP/IP[TCP 表示传输控制协议(Transmission Control Protocol)；IP 表示网际协议(Internet Protocol)]网络最初的设计目标并不是构架可运

营的网络，并且采用分组尽力转发的原则，这就导致在协议中或者设备内部没有嵌入支持网络运行、管理和维护（operations，administration，and maintenance，OAM）的要素，如设置专用的 OAM 分组或在 TCP/IP 数据分组中携带 OAM 信息等。因此，面对网络基础设施的日益复杂，TCP/IP 简单的管理和维护手段已经不能满足日益复杂的网络管理需求，需要在网络设备和软件中广泛内嵌管理元素，全面加强管理的深度。

2）管理体系方面

在管理广度上，缺乏统一的管理体系。在协议体系上，互联网协议采用平面模型，垂直方向上缺少统一的管理剖面，因此导致不同协议层次的网络管理独立运行，缺乏信息的共享和管理动作的关联，不但造成了资源浪费，而且降低了管理效率。例如，网络的核心——光网络链路层采用 SDH/SONET 协议[SDH 表示同步数字体系（synchronous digital hierarchy）；SONET 表示同步光纤网络（synchronous optical network）]，该协议具有丰富的网络 OAM 功能，如远程故障指示、发生故障时光路的自动倒换等。根据上述信息，光交换节点可以快速感知网络中其他节点的运行状态（小于 50ms）。然而，目前大多数路由器 POS/ATM 接口[POS 表示运行于 SDH/SONET 协议上的数据包（packet over SDH/SONET）；ATM 表示异步传输模式（asynchronous transfer mode）]均不使用这些 OAM 信息。IP 网络的 OAM 功能相对较弱，主要依赖路由协议的超时机制，被动发现远端的故障，导致故障的发现和处置速度较慢。在网络体系上，网络节点在管理功能方面缺乏有效协同。作为一个开放、异构和复杂的分布式系统，互联网转发平面和控制平面的功能均是分布完成的，目前分布管理实体间缺乏有效协同，从而难以有效预测异常事件，并实施主动管理。

3）管理工具方面

在管理手段上，缺乏智能的辅助工具，容易导致人为故障。目前的网络运行主要依赖管理员的手工配置。随着网络拓扑复杂性的提高，以及路由协议中策略配置和安全配置的广泛使用，网络配置对网络管理员的要求越来越高。以域间路由协议——边界网关协议（Border Gateway Protocol，BGP）为例，目前骨干网络中单个自治系统（automous system，AS）需要配置的邻居可达几百个甚至上千个，单个路由通常包含十多个路径属性，这些属性的组合十分复杂。如何理解并正确配置这些属性，确保不同边界路由节点上配置的策略互不冲突是网络管理员面临的挑战。管理员不但要为日益复杂的网络拓扑设计出合适的配置方案，还必须保证配置操作时谨慎细致，因为任何小的疏忽都可能带来网络的不稳定甚至瘫痪。例如，1997 年 4 月，美国佛罗里达州的一个小型互联网服务供应商（Internet service provider，ISP）（自治域号 7007）配置 BGP 时，允许将从 Sprint 学来的 BGP 路由作为自己的路由发布回 Sprint。Sprint 的 BGP 路由器没有过滤就将其重新发布到互

联网上。路由表信息增加一倍，并快速在互联网传播，从而导致很多路由器崩溃。2008 年 2 月 24 日，巴基斯坦电信（自治域号 17557）由于错误配置了 BGP，将一条 YouTube 前缀的子前缀向外宣告至其服务提供商电讯盈科环球业务有限公司，这条错误的路由消息在互联网上传播，引发了子前缀劫持攻击，造成路由黑洞，使得 YouTube 在全网范围内不可访问。

3. 现有网络的可生存性设计难以满足关键应用的需求

1）链路方面

物理方面的关键热点链路易于成为网络的薄弱环节，导致网络生存能力降低。分组网络本身具备一定的抗毁生存能力，只要网络拓扑保持一定的连通性，即使网络中某个节点或者链路发生故障，也能够通过路由协议的分布计算发现另外一条可用路径，从而保持整个网络的可达性。但是，目前网络冗余度较低，低冗余度所带来的直接问题就是连通性不好，由于网络的无尺度特性，关键热点链路往往成为网络的薄弱环节。2006 年 1 月 9 日，Sprint 骨干网仅仅两条链路发生故障，就导致数百万固定和移动网络用户服务中断，或者传输率大大降低。关键链路通常成为蓄意打击或破坏的对象。

2）协议方面

协议方面的域间单路径路由导致网络抗毁生存能力差、突发大流量传输能力弱。当前，互联网采用的是基于目的地单路径路由策略，从多条路径选出最好的一条路径来转发报文。单路径简化了转发表的设计，提高了网络基础设施对报文的转发处理速度，但是一旦该路径遭受物理打击发生瘫痪或产生其他故障，即使这时网络整体仍然处于连通状态，在重新计算新的路径之前，经过该故障路径的大量数据包也会被丢弃。同时，没有充分利用路径的冗余来并行传输，可能会导致网络中的某些链路成为性能瓶颈，突发的大流量很容易引起网络拥塞，降低网络整体的抗毁生存能力。

3）自愈方面

网络自愈恢复速度慢，难以实现应用无感知的链路切换。随着互联网规模的不断扩大和网络拓扑的日趋复杂，传统分布式路由计算方法的可扩展性面临严峻挑战。与此同时，作为网络管理和资源优化的强有力手段，策略路由在网络中的广泛应用进一步增加了互联网路由系统的复杂性。因此，目前域间路由系统的稳定性问题日趋严重，核心交换节点或骨干链路的故障常常导致域间路由长时间不稳定，大大降低了网络自愈的速度。有记录表明，互联网骨干路由器的瘫痪可能会造成域间路由长达十几分钟的剧烈振荡，造成大量数据丢失。因此，基于重新路由的互联网故障自愈方式难以满足应用无感知的要求。

信息基础设施对国家安全、国土安全和经济安全至关重要，但是却非常脆弱。

因此，美国 NSF 于 2006 年 4 月发布了信息安全保障研究发展规划，建议所有政府部门在其信息基础设施上实施保障网络安全和信息安全的措施。

1.2 取得的六点共识

从 20 世纪 90 年代开始，学术界便开展了一系列研究工作，并取得了很多成就。这些成就主要达成了六点共识。

1. 位置和身份分离

在 TCP/IP 网络中，IP 地址既用于位置标识又用作端点的身份标识，这种双重身份不仅限制了网络移动性，也带来一些安全问题，加大了访问控制的复杂性和难度，并在一定程度上影响了各种安全保障机制的效能。因此，在新型网络体系结构设计中严格区分位置和身份标识得到了普遍赞同。

麻省理工学院 Clark 等提出了指令转发、关联和汇合体系结构(forwarding directive association and rendezvous architecture，FARA)(Clark et al.，2003)，引入位置和身份标识。互联网工程任务小组(Internet Engineering Task Force，IETF)提出了主机标识协议(Host Identity Protocol，HIP)，HIP 在域名空间和 IP 地址空间加入了主机标识空间，传输层的连接建立在主机标识上，IP 地址仅仅用于网络层路由而不再用于标识主机身份。

2006 年 8 月，加州大学伯克利分校的 Caesar(Caesar，2007)提出扁平标识路由。扁平标识路由完全没有使用位置信息，报文头中不包括位置信息，而是直接基于标识进行路由。该方法除继承位置身份分离的优点外，还有一些独特的特点：无需建立单独的名字解析系统；报文分发不依赖数据路径之外的其他信息；标识分配简单，只需保持唯一性，无需像 IP 地址一样，既要保证唯一性又要保证与网络拓扑的一致性。

2007 年，圣安德鲁斯大学的研究人员提出了标识位置网络协议(Identifier/Locator Network Protocol，ILNP)。ILNP 将 128 位地址空间分为位置标识和身份标识两部分，高 64 位作为位置标识，命名一个子网，低 64 位作为节点身份标识。在核心网中路由时只使用高 64 位，而在高层协议维护会话状态时只使用低 64 位(Atkinson et al.，2012)。

2. 可追溯性

BAE 系统公司、LGS 贝尔实验室、洛克希德·马丁公司、约翰·霍普金斯大学等单位的研究人员都认为未来的网络体系要支持可追溯性。

BAE 系统公司的研究人员认为，未来的网络要阻止未授权的访问，记录合法

用户的访问及网络信息流，可按需审计。LGS 贝尔实验室的研究人员认为，基于硬件的设备可追溯性可以减少人为配置错误，有利于追根溯源。将基于角色的安全、设备可追溯性及位置感知有机结合可实现环境感知的动态可信。洛克希德·马丁公司的研究人员认为，未来网络应该验证用户行为是否和安全及服务质量相关的具体约定一致。

约翰霍普金斯大学的研究人员认为，在未来网络中，资源使用应该可审计，用户应该可被合适的授权机构追溯，网络用户和位置信息要对未授权实体透明。LGS 贝尔实验室的研究人员认为，在未来的网络中，网络设备、软件组件和用户对网络资源的访问必须被严格限制。在认证和授权时必须考虑物理和逻辑位置。

另外，美国斯坦福大学的 Casado 提出了企业网络的安全架构(Secure Architecture for the Networked Enterprise，SANE)体系结构(Casado et al.，2006)，采用基于集中式管理控制的全网网络实体的安全认证、接入控制、路由控制等机制以在体系结构上保障网络的安全性。在 SANE 中，端系统必须通过域控制器的安全认证来获得网络的接入权限。域控制器代理通信双方进行协商，并根据协商结果为通信双方指定路由。

3. 支持多宿主和多路径

多宿主和多路径可提高网络的生存性，抵抗拒绝服务攻击，实现负载均衡；也可防止部分路径上的信息被截获而导致信息泄露；通过适当的冗余，多路径路由还可纠正报文中的错误并回避一些路径上的链路故障，最终提高网络的生存能力。

哥伦比亚大学的研究人员认为，虽然互联网可通过将报文发往不同的中介节点，由中介节点再将报文转发到目的地的方式实现多路径路由，但无法保证路径是不交叉的，因此应该完善互联网路由方式使得数据报文可以沿多条非交叉路径进行路由。

之前的 BGP 协议针对每个目标前缀只能使用单个路由，因此在 2006 年的美国计算机协会数据通信专业组(Special Interest Group on Data Communication，SIGCOMM)会议上有研究人员提出了域间多路径路由(multi-path inter-domain routing，MIRO)协议，以提供灵活的路径选择方式。

4. 控制和数据分离

AT&T、贝尔实验室、LGS 贝尔实验室、罗彻斯特理工学院(Rochester Institute of Technology，RIT)等单位及国际电信联盟电信标准分局(International Telecommunication Union-Telecommunication Standardization Sector，ITU-T)的研究人员均认为控制和数据必须分离。控制和数据分离可避免网络用户对控制及基础设施的攻击。

贝尔实验室的研究人员认为，传输、路由交换、存储机制需要严格区分，如有可能，应尽量使其在不同的网络上运行。将具有不同要求的信令协议和传输协议分离，消除当前互联网体系结构的脆弱性，有助于安全性和可靠性。

RTI International 的研究人员认为，数据流一定不能影响控制信息的传输。在网络节点及中介的路由交换节点上，应该保证控制功能所需的处理和缓冲资源。

ITU-T 的研究人员认为，未来的网络应该分离控制、管理、传输和服务功能。

5. 网络快速自愈恢复

实现网络可靠性的前提是能够快速检测到故障。故障检测技术可分为链路检测技术和网络检测技术两大类。为了快速检测到网络故障，有学者开发一种故障检测通用服务，称为邻接对等体检查服务。该服务可以集成到现有的路由协议中，不仅可以检查物理层的可达性，也可以检查控制平面的操作状态。IETF 提出双向转发侦测(bidirectional forwarding detection，BFD)机制，对等体在所建立的会话通道上周期性地发送检测报文，如果在足够长的时间内没有收到对端的检测报文，那么认为在这条到相邻系统的双向通道上发生了故障。BFD 与路由协议的互动可以缩短路由协议链路状态检测周期，从而使路由协议更快速地收敛。

域内路由收敛较慢的原因之一是域内路由收敛过程是响应式、全局性的。因此，在没有全局收敛的情况下如何快速恢复连接是重要研究方向。有学者提出一种路由恢复方案，称为多路由配置，其允许检测到故障后在替代的输出链路上转发报文。IETF 起草了一个 IP 快速重路由框架，建议使用隧道机制处理链路和节点故障。

目前域内路由快速恢复机制相对成熟，但是如何快速检测大面积的网络故障威胁及域间快速路由恢复机制仍需要进一步研究。

6. 内在支持移动性

当前网络体系结构很难支持移动的无线网络环境。例如，如果要把移动自组织网络的数据发往互联网，那么移动自组织节点必须实现标准通用协议，但这与节点有限的资源存在矛盾。此外，未来网络中将包含大量的移动设备。网络不仅要支持设备的移动性，还要支持网络的移动性。

体系架构技术公司(Architecture Technology Corporation，ATC)的研究人员认为，在移动环境下节点的位置经常发生变化，而节点的标识应当保持不变，因此需要改变当前互联网的命名方式。伊利诺伊州立大学的研究人员也认为，未来网络需要采用支持设备移动性的新型寻址方式，并且需要支持多种移动传输技术：802.11、802.16、无线蜂窝网络等。Intel 的研究人员认为，未来网络需要支持移动节点和基础设施的简单配置，所有的移动通信设备都要能够根据事先制定的传输、

安全策略进行自我配置。智能控制系统有限公司的研究人员提出了跨层节点体系结构，目标之一是推动无线自组网的自我配置。约翰·霍普金斯大学的研究人员认为，未来网络需要综合使用数据库和目录服务、发现协议、安全零配置、安全动态接入、层次式信任、角色和责任定义等机制来支持移动性。

1.3　存在的三点争议

在取得的一系列成就中，除了达成的六点共识，还主要存在以下三点争议。

1. 简单与智能

端到端是互联网的重要设计原则，即保证网络的简单，尽量减少对上层应用的约束和限制，从而便于上层应用的发展。端到端原则是互联网取得成功的重要原因之一，但随着互联网的发展，这种简单原则面临的挑战与日俱增。

有些人认为，网络边缘防护不力是如今安全问题层出不穷的重要根源，简单网络也制约了一些上层应用和管理控制的效能。为此，人们开始重新思考端到端原则的合理性，考虑是否需要给网络增加一些智能。

有些人认为，应当在保证网络层功能不变的前提下，让网络具有更多的智能，于是人们提出了知识平面的思想。知识平面是一种特殊的覆盖网络(overlay network)，它从端节点和网络节点获取相关信息，将信息聚合后用于网络故障的检测和恢复、网络管理和控制等。

有些人认为，应当在网络层加入智能，使得网络能够感知底层链路特性、业务内容及网络实体(上层应用服务、端主机、用户身份和行为等)，以便适应多样性应用，提高网络的安全性，实现管理可视化和基于网络的安全防护。例如，SANE 提出了路由控制的思想，即不再对报文进行无条件的路由转发，而是根据发送方和接收方事先声明的通信策略，并结合路由信息完成转发。这种思想一方面加强了对路由转发的策略控制，针对每个流进行访问控制，另一方面能够为上层应用制定相应的路由转发策略，便于实现一些特殊的路由方式(如用户指定路由等)，对服务质量、移动性、多宿主、负载均衡等新技术提供很好的支持；此外，报文转发需要满足接收方的策略，可以有效防止以分布式拒绝服务攻击为代表的网络攻击，提高了网络的安全性。

还有一些人则认为，在互联网新体系结构研究中，为了支持上层应用的创新发展，端到端原则应当继续得到遵守。尽管在网络中心(如路由器)加入新的功能可以增强对高层某些特定应用的支撑，但是却破坏了网络原有的透明数据传输特性，不利于上层应用的发展和创新。同时，考虑到端系统日益增强的计算能力，为减轻网络负担，应当把一些复杂操作(如报文流检测)交给端系统处理，而不是网络。