



专题:未来网络

CoLoR 网络体系与传统互联网的一种过渡方案

胡梦春,王兆旭,罗洪斌,陈 功

(北京交通大学电子信息工程学院 北京 100044)

摘 要:针对可配置性差、用户不友好、设备存在排他性、难以支持新网络扩大部署规模等问题,提出了一种全新的网络过渡机制,力图解决 CoLoR 网络体系向现有互联网互联过渡的难题。简要介绍了该机制的研究背景、设计思路、主要技术组件及多种场景下的具体解决方案。

关键词:未来互联网;CoLoR;隧道;网关;异构网互联

doi: 10.11959/j.issn.1000-0801.2015325

An Incremental Deployment Approach from the Internet to CoLoR

Hu Mengchun, Wang Zhaoxu, Luo Hongbin, Chen Gong

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

Abstract: Focusing on poor configurability, user-unfriendliness, exclusivity, difficulty in supporting large scale deployment of new network architectures, an approach in incrementally deploying the CoLoR future internet architecture was proposed. In particular, the research background, the design principles, the main components of the mechanism and specific solutions under a variety of scenarios were described.

Key words: future internet, CoLoR, tunnel, gateway, heterogeneous network interconnection

1 引言

互联网自发明以来,取得了巨大的成功。但随着互联网的迅速发展和推广应用,它逐步暴露出了一系列架构层面的原始设计缺陷。为从根本上解决这些原始设计缺陷,业界提出了多种全新的未来互联网体系结构,如 NDN(内

容中心网络)、MobilityFirst、CoLoR。然而,新的互联网体系架构与现有互联网体系往往存在着根本的异构性,使得二者的协议兼容与数据互联成为一个亟待解决的课题。为此,本文针对北京交通大学下一代互联网互联设备国家工程实验室提出的 CoLoR^[1]新网络体系结构,设计了 CoLoR 与现有互联网实现服务级互联的方案。实现 CoLoR 新网络

收稿日期:2015-10-26;修回日期:2015-12-07

基金项目:国家重点基础研究发展计划(“973”计划)基金资助项目(No.2013CB329100),国家自然科学基金资助项目(No.62171200, No.61422101, No.61232017),教育部高等学校博士学科点专项科研基金资助项目(No.20130009110014),教育部新世纪优秀人才计划基金资助项目(No.NCET-12-0767)

Foundation Items: The National Key Basic Research Program of China(973 Program)(No.2013CB329100), The National Natural Science Foundation of China(No.62171200, No.61422101, No.61232017), The Research Fund for the Doctoral Program of Higher Education of China(No.20130009110014), Ministry of Education New Century Talent Program(No.NCET-12-0767)

论文引用格式:胡梦春,王兆旭,罗洪斌等. CoLoR 网络体系与传统互联网的一种过渡方案. 电信科学, 2015325

Hu M C, Wang Z X, Luo H B, et al. An incremental deployment approach from the internet to CoLoR. Telecommunications Science, 2015325

架构逐步兼容并替代现有互联网的过程是一个循序渐进的过渡过程,称在这种过渡过程中使用的协议兼容系统为“过渡方案”。该方案能够在有效实现新网络在面向普通用户提供数据服务的同时,大幅度降低新网络部署的成本,并确保新网络对普通用户透明,显著提升用户体验。同时,该方案的部分设计思想亦可以应用到其他网络体系的部署过程中,实现低成本的异构网互联。

2 背景

在过去的几十年间,互联网对人们的生活和生产施加了巨大的影响,极大地改变了社会的面貌。互联网的雏形——ARPANET^[2]在1970年还仅仅是一个十分简单的互联架构,但在1974–1982年制定并丰富起来的TCP/IP协议族,却出人意料地推动互联网发展成为迄今世界上最大的统一市场实体。然而,随着互联网用户及应用的快速增长,互联网自身暴露出了诸多问题,包括受限的可拓展性和较差的安全性等。不幸的是,仅仅通过在现有互联网架构上进行增补式的修改已经难以满足日益严苛的未来网络发展需求。因此,近年来针对全新架构互联网的讨论和设计方案逐步成为人们关注的焦点。

但是,在当前互联网体系上部署全新的网络架构与实现新网络与现有互联网的互联,却面临重重困难。

(1) IP网络部署规模巨大

当前互联网绝大部分由运行TCP/IP协议族的网络组成。IP网络的部署规模十分巨大,且IP对网络各个栈层的耦合度较高,以至于对IP网络进行任何有效的全局修改都几乎不能实现。20世纪最后20年,随着基于IP网络的设备大规模部署,进入了这样一个时代:全球的互联网设备和用户终端爆炸式增长,且深度依赖TCP/IP协议架构。预计至2020年,将有逾500亿台IP网络设备投入使用。其他全新的网络架构在可预见的未来,将很难替代IP网络发挥相同的作用。

(2) 互联网产业高度依赖IP基础设施

目前用户及运营商普遍使用的网络产品,硬件层面内嵌了针对IP的处理模块,软件层面使用的是基于IP的socket套接口。与互联网相关的产业链在TCP/IP协议族上形成了不可逆转的闭环,任何从整体上替代IP软硬件的尝试都将面对难以承受的资金开销。

(3) 服务数据与IP呈现高耦合度

当前互联网已经承载了绝大多数用户数据和服务内

容。新网络架构要获得用户和服务商的认可,就必须兼容当前网络中极其丰富的数据服务。然而这些服务与IP网络的解耦往往又是困难的,例如Web、FTP、流媒体等服务形式,往往架构于TCP/IP协议族之上。这导致当前互联网中的服务虽然得到了良好的推广和极大的丰富,却难以支持除IP以外的其他网络层协议。

(4) 已有的兼容方案难以推广

传统的协议兼容方案,例如用户隧道、协议转换和多重协议栈等,已在实际部署中被证明是复杂且难以配置的。某种原因是,在现有TCP/IP体系下,协议栈的设计违背了OSI参考体系“严格分层”的设计思想,TCP/IP协议栈的上下栈层之间的高度耦合性使得上层服务高度依赖下层提供的IP路由机制。

由以上得知,每一种全新设计的网络架构无论如何成长,终将直面与现有互联网体系的冲突。如果没能找到有效的兼容机制使二者并存和融合,新网络架构将长期徘徊在小规模验证和部署的程度,其发展和推广将受到限制。

3 协议兼容技术研究现状

IPv6^[3]是IPv4的替代协议。在IPv4地址资源日趋枯竭、报文字段拓展功能不足的背景下,IPv6致力于修复IP网络原有的设计缺陷,并在十余年前即已发展成熟到可推广部署的阶段。然而,IPv6花费了数十年致力于替换已经拥有庞大设备基数的IPv4,并在付出了巨大的资金、人力和软硬件开销之后,仍未能替代IPv4在互联网体系中的主体地位。时至今日,诸多IPv6的应用场景仍然需要协议切换、隧道管理等配置。这些配置步骤繁琐,协议切换麻烦,无法做到对用户透明。这导致了终端用户不愿意接受IPv6作为IPv4的替代方案。此外,IPv6在协议架构上存在排他性,与IPv4无法天然共存,这导致了网络运营商也不愿花费额外的开销去更换IP网络设备。所以,除却商业因素,对用户的不透明和与现网既存设备的冲突,是始终制约着IPv6继续推广的重要因素。

NDN^[4]是近几年快速发展的一套全新的网络架构,遵循信息中心网络(ICN)^[5]体系的设计模式,细化规定了一系列的服务获取机制并成功在小型系统上得到了验证。不幸的是,NDN不像IPv6与IPv4之间的渊源那样深厚,它与IP网络呈现了完全的异构性。NDN服务获取方式的完全改变,带来的是与现有互联网兼容上的巨大困难。近期,UCLA(美国加州大学洛杉矶分校)开发了一套基于JavaScript



库的 NDN 协议栈接口^[6]。此项成果为第三方 NDN 浏览器的开发提供了巨大帮助,但它并未能改变 NDN 需要专用的网络软件来提供专有数据服务这一事实。这意味着大量 IP 用户终端设备无法直接使用 NDN 提供的数据服务,而需要专门安装专用的浏览器甚至更换系统内核才能接入 NDN。这比 IPv6 面临的兼容困境更为严峻。除了 Web 服务需要重构,若想在 NDN 中推广现有种类更为丰富的服务样式,无论是对协议设计者,还是众多的软件公司而言,都将是一个更为巨大的、难以实现的挑战,正如 IPv6 目前面临的困境一样。

物联网(IoT)^[7]也是近年来新兴的网络体系之一。IoT 主要面向商业及工业应用,构建基于传感器和硬件自动化设备的网络体系。随着 IoT 软硬件的部署和应用获得越来越多的关注,IoT 本身在兼容性上的问题也就越来越暴露。一个客观现象是,不同的 IoT 研发实体各自为战,推出了完全异构的 IoT 设备。分属于不同公司的 IoT 组网产品使用各自独有的通信协议跨越现有互联网实现互联,却屏蔽了互联网中的普通用户。普通用户无法通过正常的数据访问方法进入这些网络获取服务,除非用户终端安装了专用的通信协议插件。这制约了 IoT 朝着用户友好、异构兼容的方向发展,也限制了 IoT 的进一步应用。

考虑到几种现有热门网络在部署过程中遇到的困难,总结出降低用户终端的配置难度、降低兼容系统的部署成本、消除异构网设备的排他性,对促进新网络融入现有互联网的进程是很重要的。然而,目前尚未见到有效的过渡方案,可以使新网络以“全新”的方式快速部署和投入业务,并对普通用户提供完全透明的数据服务。

4 CoLoR 网络架构及运行机制

CoLoR 是近年提出的一套脱离 IP、全新设计的网络架构。其设计思路完全面向未来网络的关键需求,诸如信息中心化、软件定义化、高效移动性、内嵌安全性、流量可控、支持演进与良好的可拓展能力等。

CoLoR 的核心设计元素是 3 种报文类型:查询分组、数据分组和注册分组。服务请求者向 CoLoR 网络发出查询分组来描述并请求一块数据或一种内容服务,网络中的服务器或缓存节点收到查询分组后,会将服务数据封装进数据分组,并沿着查询分组的转发路径原路返回送达请求者。注册分组是服务发布节点向 CoLoR 网络通告服务内容的专用报文格式,CoLoR 网络的服务解析系统通过注册分

组来获知网络中的数据服务的具体信息和所在位置。CoLoR 网络中的服务解析系统称为资源管理器(RM)。

CoLoR 网络以自治域为组织单位,每个 CoLoR 自治域拥有一台逻辑上集中的 RM,通过接收注册报文来获知并通告域内/域外所能提供的数据服务,并引导查询报文到达该请求服务的提供者。不同 CoLoR 域内的 RM 联合组成 RM 服务解析系统,通过 RM 间的通告和协商完成服务的跨域注册和 CoLoR 其他功能策略的制定。RM 服务解析系统的主要功能类似于现有 IP 网络中的域名解析系统(DNS)^[8]。而更多的,RM 系统同时还承担了诸如域间流量均衡^[9,10]、主动拥塞控制^[11]、软件定义网络(SDN)^[12]等现有 IP 网络难以有效实现的丰富功能。

一个 CoLoR 网络基本运行流程的范例如图 1 所示。

首先,持有服务内容的节点 A 向本域的 RM1 注册服务标识 SID(service ID),随后 RM1 将向它的上级域注册这一 SID。当 RM3 收到来自 RM1 的 SID 注册信息时,它就会在注册表里为这个 SID 存储一个实体。另外,它也会向上级 RM6 进行注册。当 RM6 收到注册信息时,它将在自己的注册表里为这个 SID 存储一个条目。若节点 B 也持有与节点 A 相同的服务内容时,同理节点 B 先向本域的 RM2 注册 SID。随后,当 RM3 从 RM2 收到相同 SID 的注册信息时,RM3 发现自己已经有了关于这个 SID 的注册信息,但是已有的注册信息是来自 RM1 而不是 RM2,因此,它也会向自己注册表里添加一个条目。需要注意的是,此时 RM3 并不向 RM6 发送注册信息,因为它已经注册过这个 SID 了。

当一个客户端希望获取名为 SID 的服务时,它将发送一个查询(get)分组给它本域的 RM。这个查询分组应该包含想要获取的 SID 和客户端的节点标识(NID)。如果拥有这个 SID 的节点与 RM 在相同的域内,那么 RM 会根据本域的路由机制将查询分组直接转发给这一节点。如果这个节点在其他的域内,即本域的 RM 查询不到关于这个 SID 的条目时,首先,基于本地的政策,它将会选择一个上级 RM,然后选择一个能到达上级 RM 的 PID,最后将选择路径的 PID 添加到查询分组里并将查询分组发送给上级 RM。

假设节点 A 和节点 C 已经将 SID 注册好。当节点 C 想要获取这个内容,那么它将发送一个查询分组给本地的 RM4。RM4 收到后,它找不到 SID 的条目信息。因此,它就在查询分组中添加域间路径标识 P4 并把它发送给上级 RM5。同样当 RM5 收到查询分组后,它也不能找到与这个 SID 匹配的条目,同理它就在查询分组中添加域间路径标识

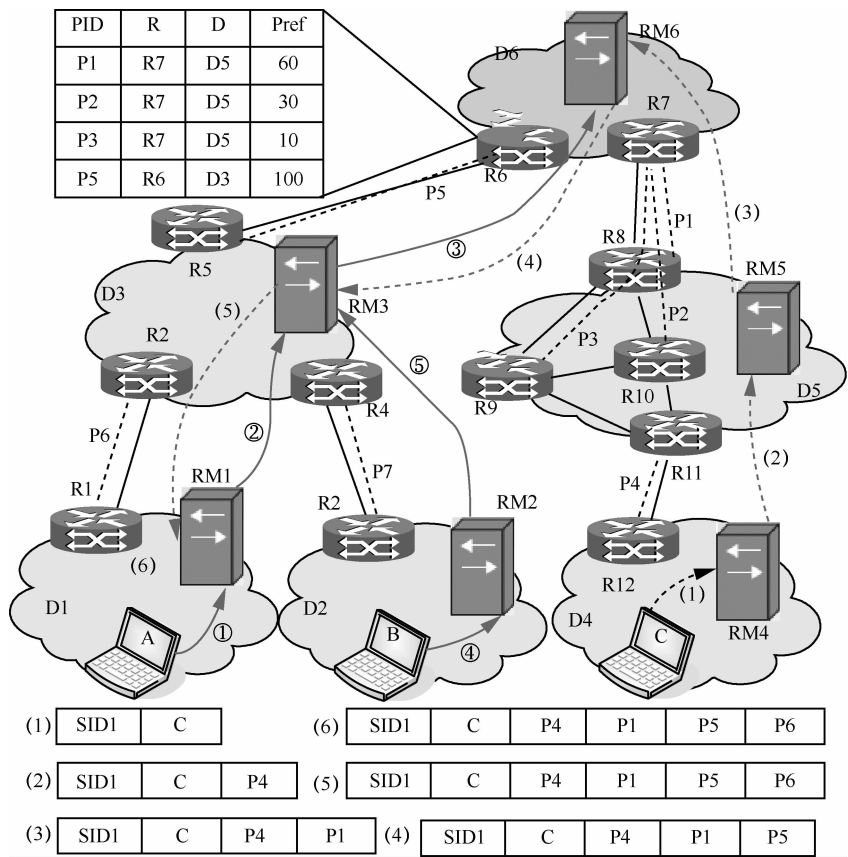


图 1 CoLoR 中注册、查询及响应数据流程

P1(或者 P2、P3)把它发送给上级 RM6。当 RM6 收到查询分组后,它在注册表里找到这个 SID 匹配的条目信息,但是由于 RM6 与 RM3 不在同一个域内,它就在查询分组中添加路径 P5 并把它发送给 RM3。因为 RM3 能找到两条信息,所以它根据当地的政策选择了一条指向 D1 域的条目,并在查询分组中添加域间路径标识 P6 后把它发送给 RM1。当 RM1 收到查询分组后,发现本地的一个节点持有所需的服务,把查询分组发送给了节点 A,整个服务请求过程完成。

当查询分组发送到主机 A 后,主机 A 知道了主机 C 请求的服务信息 SID1 以及到达主机 C 的 PID 串。这时将主机 C 的 NID 以及相应路由信息封装进去,并发送到上一级域。然后由 RM1 通过边界路由 R1 转发到上一层域,同时去除 data 分组两域之间的 PID。依此类推,最终的 data 分组就会被发送到主机 C 中。

由上可以看出,CoLoR 具备传统 IP 网络不具备的诸多优势,如高效获取资源、良好的路由兼容性、域间可控性等。然而 CoLoR 也因此呈现与传统 IP 网络完全异构的机制和形态,双方在服务数据的共享上存在困难。这使得

CoLoR 需要专门的机制来解决异构网服务兼容的问题。而且在 CoLoR 的设计上,必须将协议兼容性作为一个重要方面纳入设计考虑。

因此,下文将主要描述基于 CoLoR 新网络特点而设计的一套专门与现有 IP 互联网实现服务级兼容的过渡方案。在该方案的框架下,设计了可使 IP 网络在服务层兼容 CoLoR 网络的方法,一些设计方案还可以方便地拓展到其他新网络的过渡方案中。

5 过渡场景解决方案

本节将介绍如何部署 CoLoR 过渡方案并使 CoLoR 网络同 IP 网络实现低成本互联,如何使 CoLoR 网络对 IP 接入用户完全透明以及如何基于 CoLoR 向用户提供协议无关的服务数据。同时,该过渡方案不仅能够满足普通 IP 用户的接入和服务需求,而且一定程度上实现了与协议无关的数据服务,支持安装纯 CoLoR 协议栈的新用户自由接入网络并获取数据服务。

新网络架构对现有互联网的兼容性按照栈层功能划分^[3],可分为两种层面的兼容性。



(1)网络层兼容性

即路由共存。CoLoR 自治域内部的网络层对所有路由协议开放,可以兼容 IPv4、IPv6、MPLS、Segment Routing 等现有的路由转发协议。故 CoLoR 在网络层上天然具备良好的兼容性,可与现有诸多路由协议共存并融合为一体。

(2)服务层兼容性

即数据服务的通用性。传统的数据服务兼容做法(例如用户隧道、协议转换和多重协议栈等)已在实际部署中被证明是复杂而难以配置的。用户体验是检验一种服务兼容机制是否有效的重要参考。较差的用户体验常常来源于异构网环境中复杂的接入设置和贫乏的服务资源。

为了解决服务层兼容性的问题,充分利用 CoLoR 天然支持网络层兼容性的优势,本文设计了一套无需用户参与配置的数据服务兼容系统。其核心思想是不对用户做任何前提设定或额外配置,转而在用户接入路由设备、域边界设备、IP 网络中的 DNS 体系和 CoLoR 网络中的 RM 解析系统上部署不同的技术组件,合成一套内嵌于网络架构中的兼容系统。这种方案最大的优点在于对用户透明。对用户透明也就意味着,CoLoR 作为一个新的网络架构能够以与 IP 网络平等的地位向用户提供数据服务,而不造成修改网络架构所需的额外开销,从而促进新网络的演进和推广。

根据用户的自身类型、接入需求和网络架构的组织形式,将 CoLoR 网络与 IP 网络之间可能出现的互联关系分为 4 种场景,逐一讨论并提出解决方案。

5.1 场景一:IP 网络的接入方案

在该场景下,用户位于传统 IP 网络中。此时,按照用户持有的协议栈划分为两种情况:仅安装 IP 协议栈的用户和仅安装 CoLoR 协议栈的用户。无论何种用户,当他接入 IP 网络时,要求他既能够自由访问现有互联网数据资源,

又能通过在普通浏览器上输入 CoLoR 专有域名来访问 CoLoR 网络中的数据资源。为了实现这个目标,在用户接入网关和域边界代理网关上分别安装了 DNS 重定向组件和隧道组件。

(1)IP 用户接入 IP 网络

在用户接入网关和互联网 DNS 解析服务器上部署了 CoLoR 域名分类模块。该模块上注册了 CoLoR 网络面向互联网的若干 Web 代理网关的域名和地址,用户在普通浏览器上输入代表 CoLoR 网络的域名即可自动访问 CoLoR 网络中的数据。

此外,针对互联网中的某个数据块,如果 CoLoR 域内拥有对该块数据的缓存副本,亦可以将代表该数据块的 URL 请求重定向到 CoLoR 边界网关处。这样,就拓展了 CoLoR 作为一个互联网自治域的作用,可充分利用自身作为 ICN 架构的信息中心特性,为当前互联网提供高效的缓存备份和访问加速服务。

该场景解决方案如图 2 所示。

(2)CoLoR 用户接入 IP 网络

使用纯 CoLoR 协议栈的用户,如果是向 CoLoR 域发出数据请求,则接入网关需要通过 CoLoR 边界网关构建 IP 隧道的方式,将 CoLoR 用户发出的查询分组发往 CoLoR 域并使用这个隧道回送数据分组,如图 3 所示。

如果该用户希望从当前互联网获取服务数据,则有两种解决方案。其一,视该接入网关请求功能的丰富程度而定,识别该用户查询分组中服务标识字段中包含的 URL 信息,即可充当反向代理的功能,接入网关以 IP 为用户获取互联网数据并在本地组装成 CoLoR 协议下的数据报文回送给用户,如图 3 中“IP 代理流 1”。其二,为了避免接入网关的设计过分臃肿,CoLoR 用户面向 IP 网络发出的服

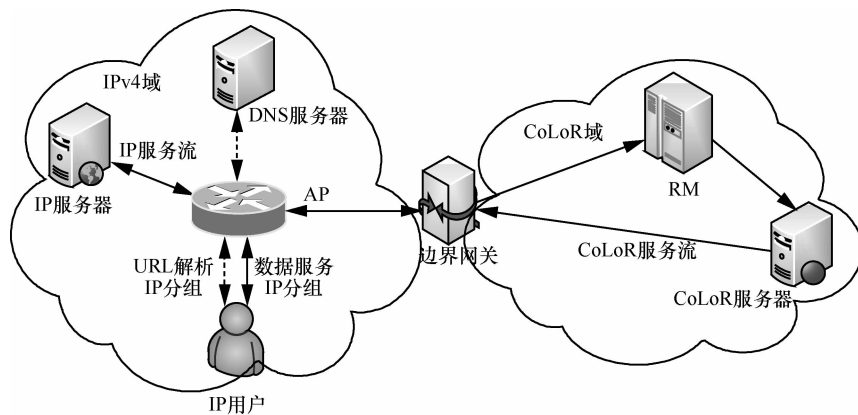


图2 IP用户接入IP网络

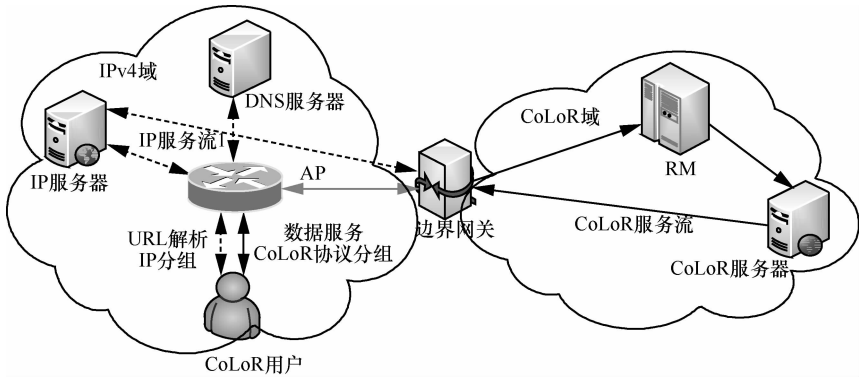


图 3 CoLoR 用户接入 IP 网络

务请求可以通过 IP 隧道统一转交给 CoLoR 边界代理网关代为处理,并将获取到的数据组装成用户可识别的 CoLoR 数据报文沿着 IP 隧道原路返回,如图 3 中“IP 代理流 2”。

5.2 场景二:CoLoR 网络的接入方案

在此场景中,用户接入 CoLoR 网络中。与场景一类似,接入用户仍分为 IP 用户和 CoLoR 用户两类。

(1)CoLoR 用户接入 CoLoR 网络

CoLoR 用户本身可以很方便地向 CoLoR 网络请求服务,而当该用户希望获取 IP 网络中的资源时,与场景一相同,用户发出的查询分组将由 RM 定位到边界代理网关处,

后续数据获取的工作由边界网关代为处理,如图 4 所示。

(2)IP 用户接入 CoLoR 网络

一方面使用 IP 转 CoLoR 的接入网关使用户的报文顺利地接入 CoLoR 的 RM 解析体系,另一方面在接入网关上部署了 DNS 末端服务器,并通过 CoLoR 自动隧道与互联网 DNS 解析体系相连接。这样,IP 用户即便接入了 CoLoR 的网络,也不需要做任何额外配置,即可方便地同时访问传统互联网和 CoLoR 新网,如图 5 所示。

5.3 场景三:CoLoR 报文穿越 IP 网络的互联方案

当两个 CoLoR 自治域部署在地理上相互远离的两个

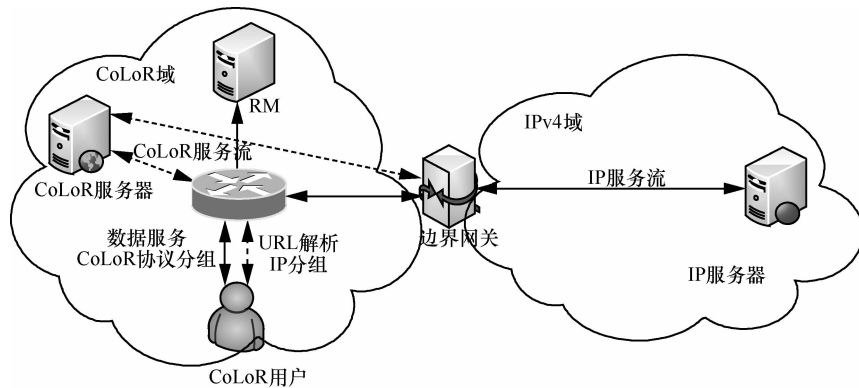


图 4 CoLoR 用户接入 CoLoR 网络

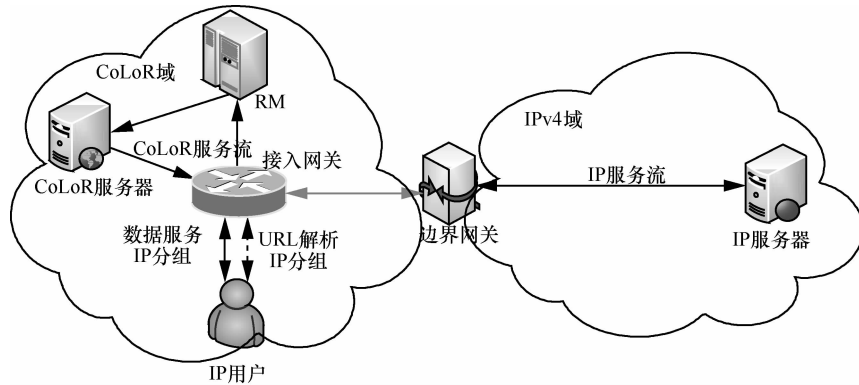


图 5 IP 用户接入 CoLoR 网络



位置,根据目前互联网的部署情况,需要跨越 IP 网络实现两个 CoLoR 自治域的互联。这种互联的基本要求是,跨越其间异构网络的过程需要对远程互联的双方自治域透明。这需要两个 CoLoR 自治域连接 IP 网络的边界路由器能够自动识别不同目的地报文和相应地创建 IP 隧道,如图 6 所示。

5.4 场景四:IP 报文穿越 CoLoR 网络的互联方案

场景四同场景三类似。当两个 IP 自治域部署在地理上相互远离的两个位置,而中间由 CoLoR 网络相连时,IP 报文同样需要跨越 CoLoR 网络实现互通,如图 7 所示。

6 过渡方案部署进展

本节针对场景一和场景二开发了验证系统,介绍了实现的技术组件和具体运行机制。

6.1 技术组件

场景一、二为用户接入场景,其设计目标是令用户完全脱离协议兼容的配置手续,即无论持何种终端协议的用户接入何种网络,均可以在无需任何额外配置的情况下,方便地访问到包含 IP 和 CoLoR 在内的全网服务资源。为

了实现这个目标,将兼容系统分为 4 种主要的技术组件:隧道组件、DNS 重定向组件、用户接入网关和边界代理网关。具体设计与实现如下。

(1)隧道组件

隧道组件是用户接入场景中最关键的组件,它直接承载了使用异构网络协议的用户收发的服务流,可支持用户无障碍地接入异构网自治域中。一个特定 CoLoR 域中的隧道将承载所有来自异构网的用户和服务数据。与传统隧道机制不同的是,依托于 CoLoR 架构的网络层无关特性,关于隧道的所有构建工作将在部署 CoLoR 协议的接入网关、域边界路由器和 RM 中进行。隧道的两端出入口仅限于接入网关和域边界路由器来维持,而隧道的管理任务将交由本域内的 RM 执行。用这种方法,基于隧道的兼容系统就可以正常运行于 CoLoR 网络架构中,同时保持对用户透明。

如图 8 所示,使用 click 软件路由器与原始套接字,在两个 CoLoR 域上构建了隧道组件,两个 CoLoR 域间由两个域间路径标识(PID)连接。如同传统 IP 隧道一样,需要使用 CoLoR 报头来封装原有的异构网报文,这里选择数据

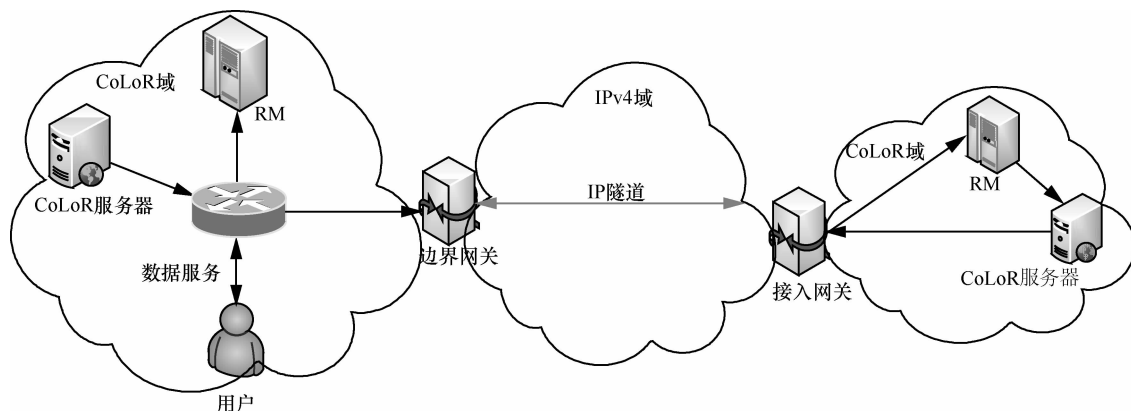


图 6 CoLoR 报文穿越 IP 网络

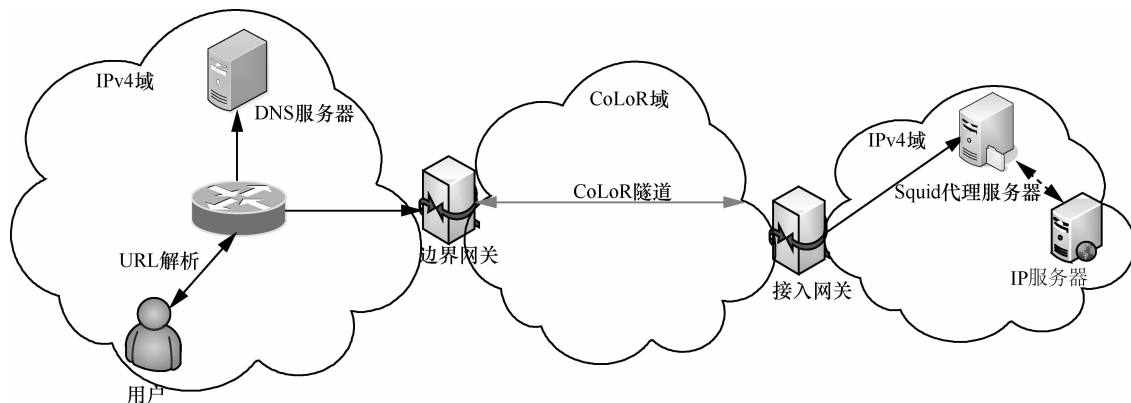


图 7 IP 报文穿越 CoLoR 网络

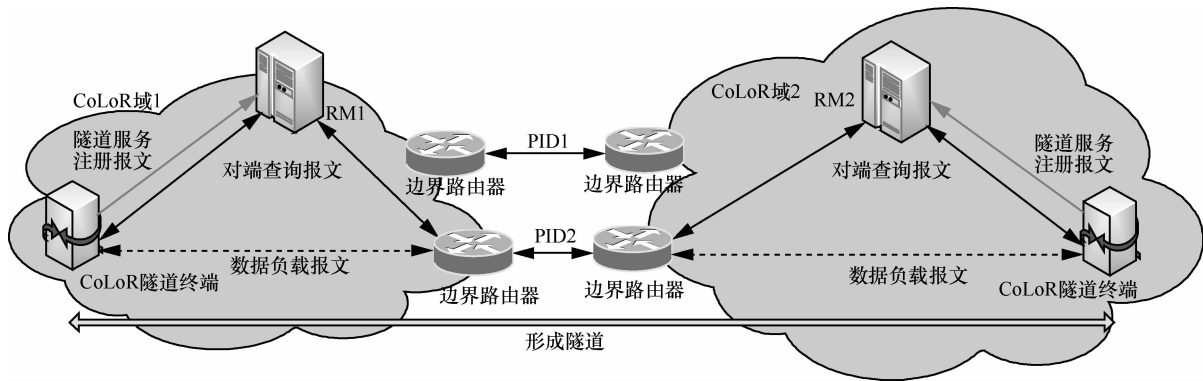


图 8 隧道组件基本机制

报文来封装和承载隧道的信息流,并构建双向通路。数据报文实现双向转发的前提是隧道双端都知晓到达彼此所需的 PID 信息。故还需要隧道双端的设备向 RM 注册各自的隧道服务信息(即隧道 SID)并各自定期向 RM 系统发出请求对方隧道 SID 的查询报文。通过查询报文的相互收发,隧道双端设备即可定期维护与更新 CoLoR 域间可用 PID 的信息,确保在 PID 不断变化的情况下,隧道能够跨越多个 CoLoR 域维持长期的连接。

使用这种 CoLoR 隧道组件承载了 IP 网络中的 TCP 流,并实现了网页传输的隧道封装。通过测试隧道对 Web 服务的承载实验,验证了 CoLoR 构建的隧道可以支持普通 IP 用户正常的访问需求。还通过还原 TCP 在带宽占用上的典型行为,验证了 CoLoR 隧道可以支持对传统 TCP 服务的线性传输。

如图 9 所示,使用原始套接字实现一条单一的隧道,并承载了多个客户端的网页服务请求。分别测试了客户端的有线接入链路和无线接入链路两种链路环境,并将结果与用户不使用隧道直接发起网页服务请求的情况进行对比。由图 9 可知,网页载入时延略有提高是由于 TCP 服务流受到了隧道报文封装与解封机制的作用,但时延的改变

并不显著。故隧道的存在没有对 IP 用户正常的网页访问性能产生显著的扰动,正常 Web 服务的用户体验不会因隧道的存在而发生明显降低。此结果可以验证,该隧道组件的设计机制能够正常支持 IP 网络服务流的传输。

如图 10 和图 11 所示,随着 IP 客户端数量的增加,在它们共享的隧道中出现了带宽瓶颈。总下载速率在客户端数量增至 3~4 台时不再显著增长,意味着此时隧道中的带宽接近满载。与此同时,隧道分组丢失率却不再显著增长。这符合传统 TCP 流在占用带宽上的行为特征:尽管 TCP 流数量的增加导致了其共享瓶颈链路上的带宽发生了满

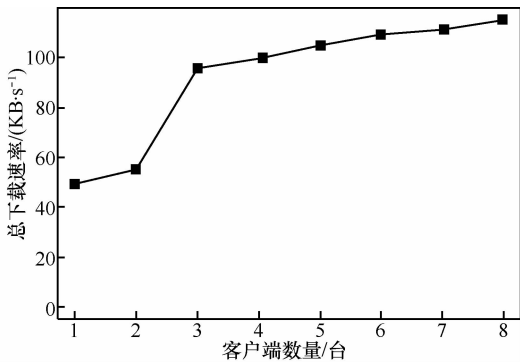


图 10 隧道环境下多客户端 Web 服务下载速率

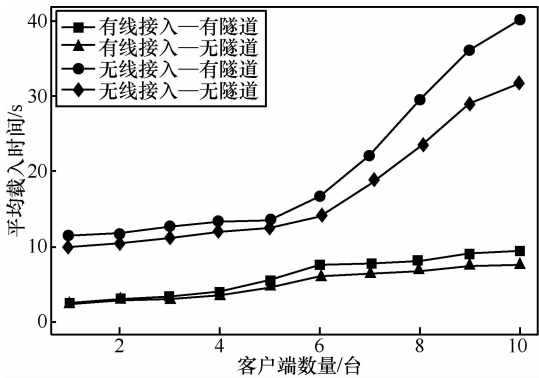


图 9 隧道环境下网页平均载入时间

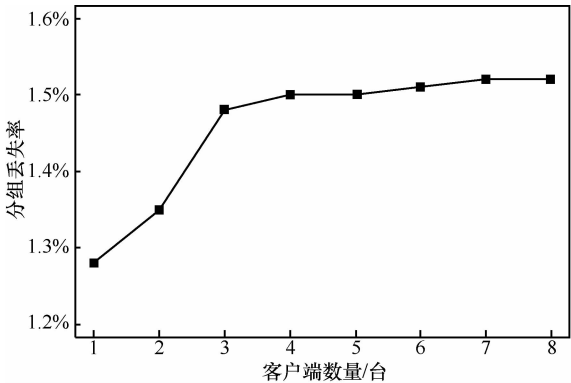


图 11 隧道环境下多客户端 Web 服务的隧道分组丢失率



负荷的现象,但分组丢失率却没能随着客户端的增加而继续增长。这是因为,TCP对丢失分组十分敏感,丢失分组会导致TCP发送窗口长度的减小,进而限制了每条TCP流的实际吞吐量。所以TCP在瓶颈链路发生拥塞的情况下,并不是通过增加丢失分组,而是通过限制窗口大小来限制单条流的吞吐量。由此可以得出结论,CoLoR隧道真实地反映了传统TCP的流行为,证实了隧道本身的带宽、丢失分组等性能参数是线性、稳定和可预测的,这与IP网络下传统隧道的特性相一致。

(2)DNS重定向组件

DNS劫持是一种沿用至今且行之有效的攻击手段。攻击者通过篡改DNS服务器中某些正常域名的注册IP地址,误导正常的DNS请求定位到攻击者自己设定的错误IP地址上,使用户的Web访问获取到原不属于该域名的网页信息。现在借鉴这种攻击方式的原理,解决低成本互联CoLoR新网和IP旧网的问题,并实现IP用户向异构网自由请求服务数据。尝试通过向DNS服务器注册额外的解析地址,构建CoLoR新网络边界代理面向普通IP用户的服务链路。

基本方案是允许希望接入新网络的旧IP网络用户向DNS服务器正常发送URL解析请求,并将DNS请求分类的重定向工作交由DNS服务器处理。在当前的互联网中,

DNS可以将URL服务请求定向到普通的IP服务器,也可以将其重定向到CoLoR新网的Web边界代理网关上。

因此,借鉴了DNS劫持的原理,却不劫持域名。根据用户或服务商的需求,将URL请求重定向到CoLoR网络,并把剩余的服务任务交由CoLoR网络与IP网络边界的代理网关来完成,如图12所示。

(3)用户接入网关

指分别安装在IP网络接入端和CoLoR网络接入端的两种终端接入设备。其一端是用户终端设备,另一端则是其所处的网络自治域。用户接入网关的主要任务是同时支持两种用户的接入需求:使用纯IP协议栈的传统用户和使用纯CoLoR协议栈的新用户。两种用户均可能在IP网络或CoLoR网络中接入并向全网发送数据服务请求。接入网关需要识别这两种用户,并使用隧道和DNS组件将不同的用户请求转发至正确的目的地,如图13所示。

(4)边界代理网关

以提供Web服务的边界代理网关为例,它部署在CoLoR网络和IP网络的交界处。该网关在一个方向上通过构建标准的Web服务流,向IP网络中的用户呈递CoLoR网络内部的服务数据;另一个方向上通过联合接入网关构建隧道机制,向CoLoR网络中的用户提供IP网络中的数

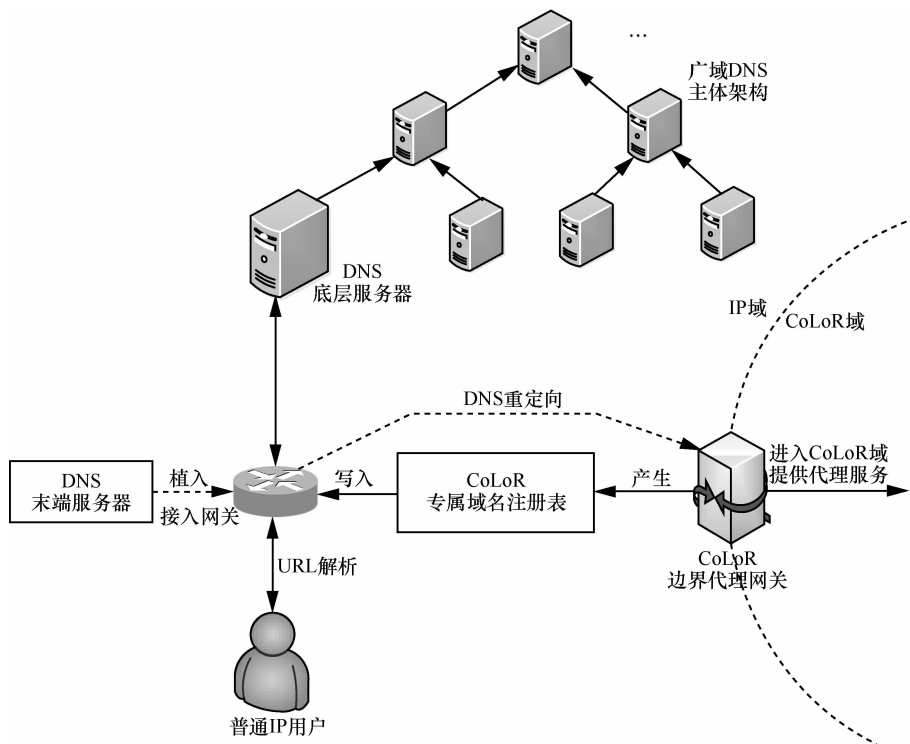


图12 DNS重定向组件的基本机制

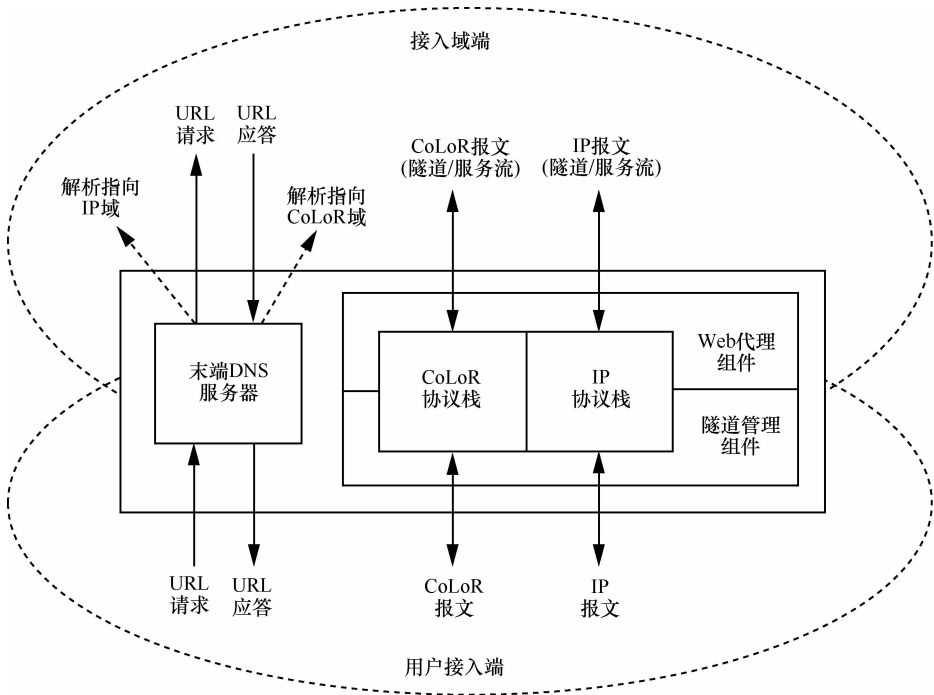


图 13 用户接入网关基本机制

据资源。网关的一端是面向 IP 用户的普通 Web 服务器,而另一端则运行了标准的 CoLoR 服务获取机制。在实际部署中,采用 Squid^[14]为基础架构开发了该边界网关,其运行原理如图 14 所示。

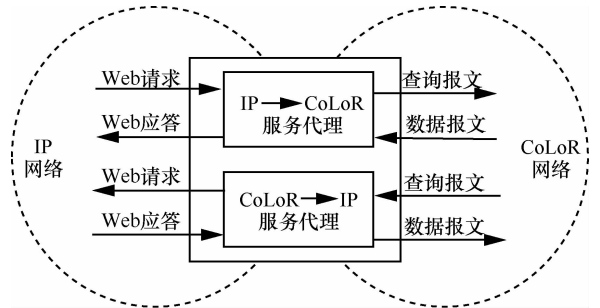


图 14 边界代理网关基本机制

由以上 4 种技术组件可知,过渡方案并不需要像 NDN 那样,在用户终端安装新的操作系统内核,或安装专属的协议栈调用库。仅需要在现有互联网关键设备上做有限的修改即可部署协议兼容系统。目标即将其设计成为一套内嵌在网络体系架构中的机制,实现对用户的完全透明。

6.2 运行机制

根据用户、接入网络、目标网络三者的不同协议组合,将场景一、二中的用户接入场景细化为 8 种访问机制。在这 8 种访问机制中,具体给出了用户从发出服务请求到最终获取服务数据的整个业务流程。

(1)场景一(a)IP 用户接入 IP 网络,访问 IP 网络中的服务数据

图 15 为当前互联网中自有的 Web 服务访问机制,作为过渡方案机制的对照。

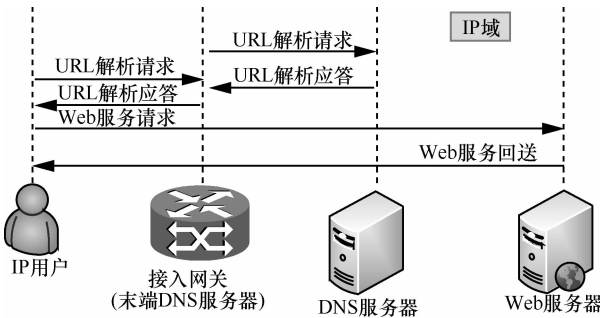


图 15 IP 用户接入 IP 网络,访问 IP 网络

(2)场景一(a)IP 用户接入 IP 网络,访问 CoLoR 网络中的服务数据

如图 16 所示,IP 网络中的接入网关安装了 DNS 重定向组件,直接面向接入的 IP 用户提供 CoLoR 专属域名的识别和解析服务。此举可尽快将 IP 用户发出的 CoLoR 数据请求识别出,并引导到 CoLoR 边界网关处进行处理。应用该机制,拥有庞大基数的 IP 网络用户无需任何终端配置,即可通过在普通 TCP/IP 浏览器上输入包含 CoLoR 代理网关域名的 URL 地址,方便地获取 CoLoR 网络向全网提供的数据服务。

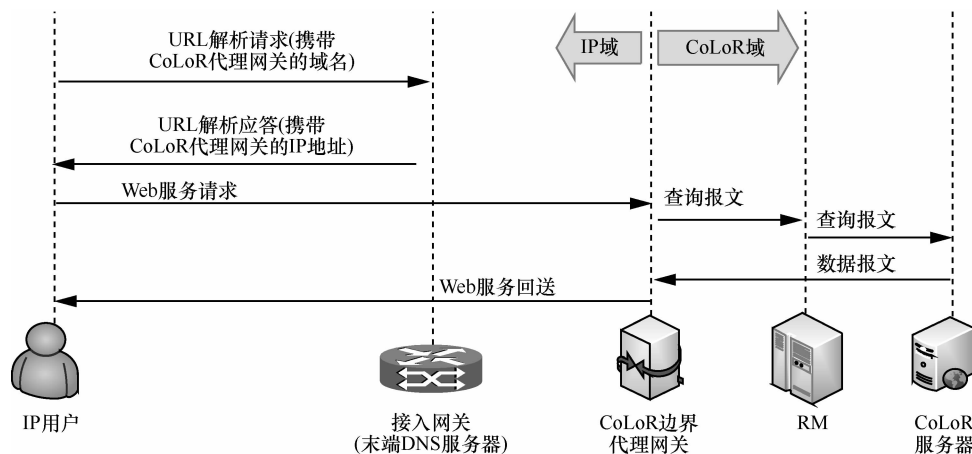


图 16 IP 用户接入 IP 网络,访问 CoLoR 网络

(3)场景一(b)CoLoR 用户接入 IP 网络,访问 IP 网络中的服务数据

如图 17 所示,CoLoR 边界网关不仅承载了双方网络的服务级代理和缓存的工作,还承载了来自双方网络异构接入用户的服务代理工作。代理网关可以方便地为接入异构网的用户提供远程代理服务。在此例中,CoLoR 边界网关承担了接入 IP 网络中的 CoLoR 用户访问 IP 网络数据服务的代理任务,可谓异构用户与异构网络之间的“桥梁”。此举省却了在用户端部署冗余多重协议栈的麻烦,避免了“胖终端”问题的发生。应用该机制,在 CoLoR 网络的后续验证与部署中,安装了全新 CoLoR 协议栈的用户设备即使不具备 TCP/IP 协议栈,也可以方便地接入广域互联网,并从中获取丰富的服务数据。

(4)场景一(b)CoLoR 用户接入 IP 网络,访问 CoLoR 网络中的服务数据

如图 18 所示,IP 网络中的接入网关和 CoLoR 边界网关之间构建了 IP 隧道,而并非 TCP 隧道。此举减小了隧道

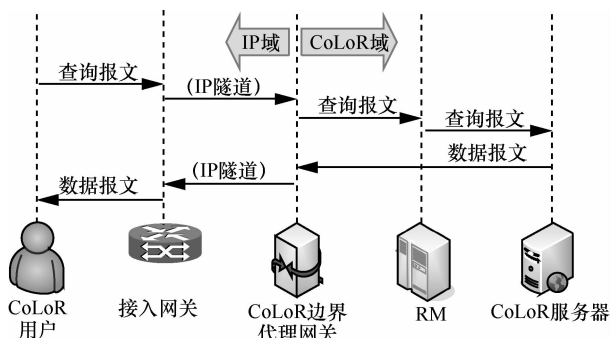


图 18 CoLoR 用户接入 IP 网络,访问 CoLoR 网络

配置的复杂度,更方便在设备之间自动建立和管理。该隧道承载了 CoLoR 用户收发的异构报文,使其顺利穿越 IP 网络与 CoLoR 网络边界网关建立通信。应用该机制,安装了全新 CoLoR 协议栈的用户设备即使不具备 TCP/IP 协议栈,也可以从广域互联网的任意一点接入,跨越 IP 网络访问并获取来自 CoLoR 域内的服务数据。

(5) 场景二 (a)CoLoR 用户接入 CoLoR 网络,访问 CoLoR 网络中的服务数据

图 19 为 CoLoR 架构的基本设计中自有的数据获取机制,作为过渡方案其他机制的对照。

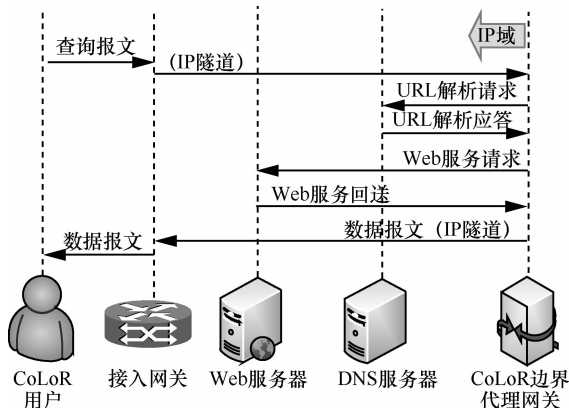


图 17 CoLoR 用户接入 IP 网络,访问 IP 网络

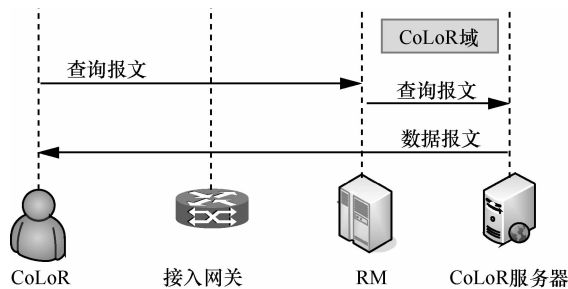


图 19 CoLoR 用户接入 CoLoR 网络,访问 CoLoR 网络

(6)场景二(a)CoLoR 用户接入 CoLoR 网络,访问 IP 网络中的服务数据

如图 20 所示,在此例中,CoLoR 边界网关是一台全功能的“CoLoR 访 IP”代理设备,一切来自 CoLoR 网络的数据请求,在网关处都将被翻译成 IP 网络下的请求报文并发往 IP 网络;同时,一切来自 IP 网络的服务数据流,在网关处将得到全权代理。IP 服务数据在边界网关处得到校验、拼接、重新分片,封装入 CoLoR 报文之后,使用专属于 CoLoR 的应用层协议回传给 CoLoR 用户。应用该机制,仅在 CoLoR

本地网络中接入的 CoLoR 终端设备,不需要额外安装 TCP/IP 协议栈即可直接向 IP 外网请求所需的服务数据。

(7)场景二(b)IP 用户接入 CoLoR 网络,访问 CoLoR 网络中的服务数据

如图 21 所示,IP 用户在 CoLoR 网络中发出的数据请求将全部交由边界网关代理。所有协议翻译、数据拼接、封装和解封装的步骤也都在边界网关处完成。在此例中,IP 用户与外界唯一的通信链路即接入网关与代理网关之间构成的 CoLoR 隧道组件。应用该机制,在 CoLoR 网络的后

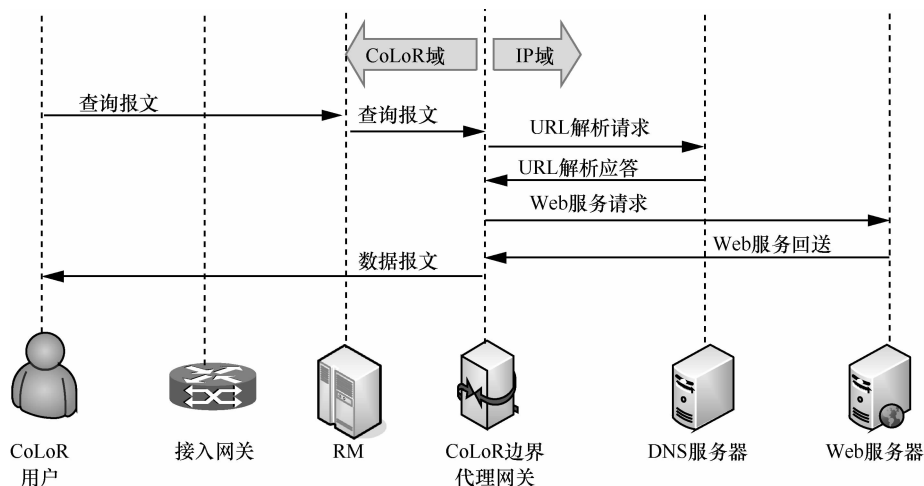


图 20 CoLoR 用户接入 CoLoR 网络,访问 IP 网络

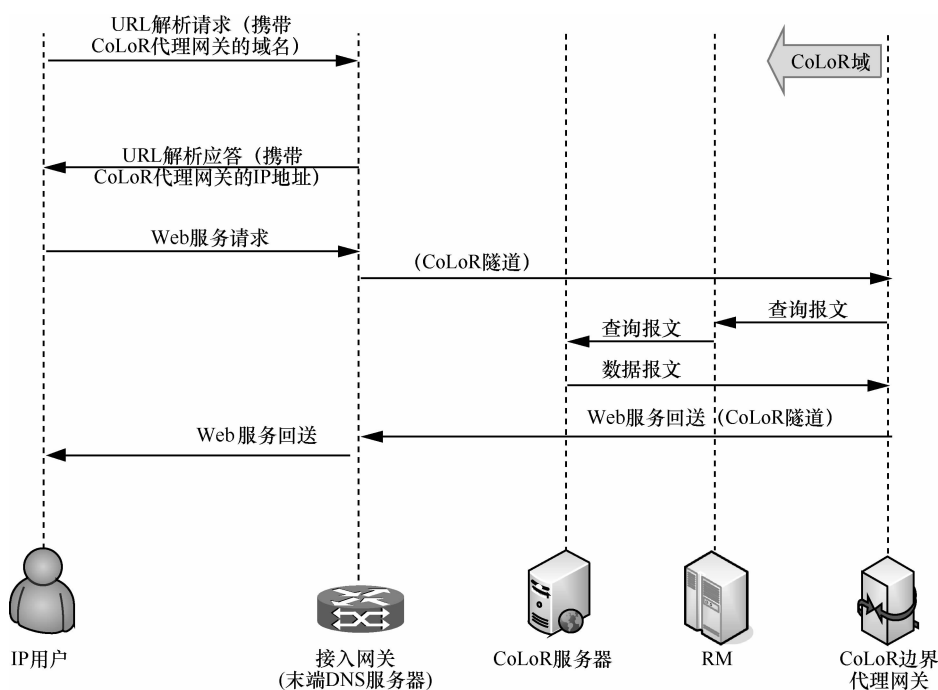


图 21 IP 用户接入 CoLoR 网络,访问 CoLoR 网络

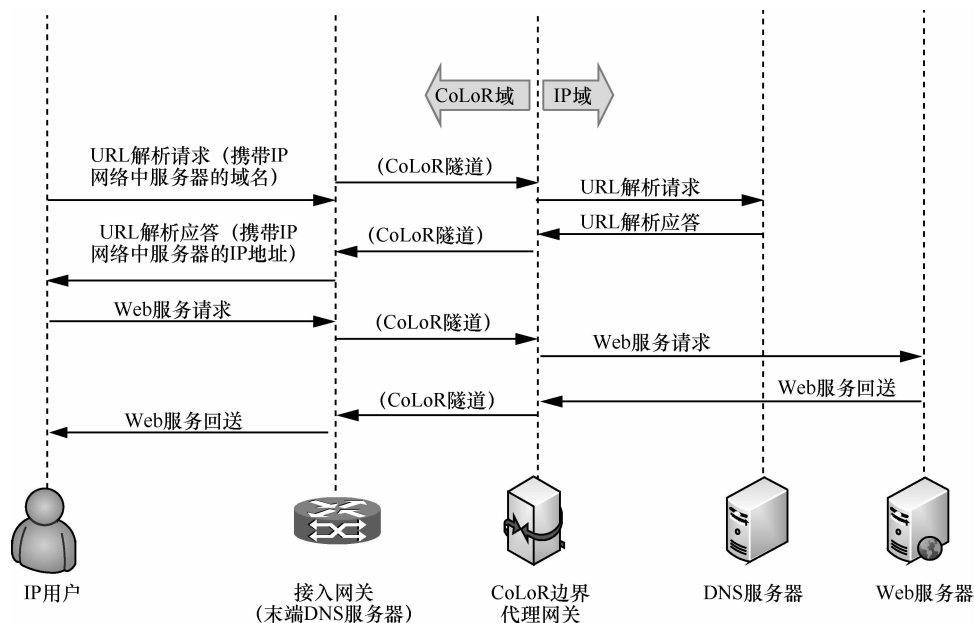


图 22 IP 用户接入 CoLoR 网络,访问 IP 网络

续验证与部署中,不需要所有接入 CoLoR 网络的用户都是 CoLoR 设备,直接使用 IP 设备也可以完成对 CoLoR 本地数据的获取。

(8)场景二(b)IP 用户接入 CoLoR 网络,访问 IP 网络中的服务数据

如图 22 所示,IP 用户在 CoLoR 网络中同样使用 CoLoR 隧道组件与边界网关建立通信,并借由边界网关实现与 IP 网络的连接。应用该机制,当未来 CoLoR 网络实现商用部署,普通 IP 用户可以在完全不知晓接入网络类型的情况下(即便恰好接入到了 CoLoR 网络中),也可以无障碍地访问到现有互联网的所有资源。

综合 8 种具体的用户接入情境,可以认识到,通过为用户接入网关和异构网边界网关部署全功能的解析、转接和隧道组件,即可做到新网络的快速推广部署。尽管部署全功能的网关与代理设备本身具有一定的难度,设备的负载能力也有待验证和优化,但该方案首次成功实现了对用户透明的协议兼容系统,绕过了异构网设备排他性的难题。可以看到,该方案在部署成本、复杂度和用户接受程度等方面,较当前其他的兼容方案拥有巨大的优势。

7 结束语

本文首先介绍了新网络架构部署过渡方案的研究背景与现状,并简要分析了导致现有过渡方案各种严重不足的主要根源。在此基础上,本文以 CoLoR 新网络体系在当

前基于 IP 的互联网上部署和互联的过渡方案为例,介绍了低成本部署新网络,并向用户提供协议无关的数据服务的设计原理和行为数据。同时,本文还列举分析了新网络过渡方案一般面对的几种过渡场景,并逐一给出了兼容系统部署的解决方案。

然而,围绕新网络过渡方案的课题,仍然有许多亟待解决的问题。例如,网关类设备作为协议兼容的骨干设备,其设计方案能否胜任实际部署中的负载需求;CoLoR 的隧道组件在域间路径标识频繁变动的情况下,如何维持稳定的传输;用户的移动性支持如何设计,都是后续研究内容。

参考文献

- 1 Luo H, Chen Z, Cui J, *et al.* CoLoR: an information-centric internet architecture for innovations. Network IEEE, 2014, 28(3): 4~10
- 2 Hauben B M . History of ARPANET. <http://pages.infinit.net>, 2010
- 3 RFC 2460. Internet Protocol, Version 6 (IPv6) Specification, 1998
- 4 Named Data Networking (NDN) Project, 2010
- 5 Xylomenos G, Ververidis C N, Siris V, *et al.* A survey of information-centric networking research. IEEE Communications Surveys & Tutorials, 2014, 16(2): 1024~1049
- 6 Lera A, Morabito G, Atzori L. The social internet of things. Proceedings of IEEE International Conference on Cloud Engineering, New York, NY, USA, 2015
- 7 Shang W, Thompson J, Cherkaoui M, *et al.* NDN.JS: a JavaScript client library for named data networking. Proceedings

- of IEEE Conference on Computer Communications Workshops, Turin, Italy, 2013
- 8 Mockapetris P V. Domain names: concepts and facilities. Std Rfc Usc/information Sciences Institute, 1983, 21(6):513
 - 9 Feamster N, Borkenhagen J, Rexford J. Guidelines for interdomain traffic engineering. ACM SIGCOMM Computer Communication Review, 2003, 33(5):19~30
 - 10 RFC3272. Overview and Principles of Internet Traffic Engineering, 2002
 - 11 Faber T. ACC: active congestion control. IEEE Network, 1998, 12(3)
 - 12 Raghavan B, Koppnen T, Ghodsi A, *et al.* Software-defined internet architecture: decoupling architecture from infrastructure. Proceedings of Acm Workshop on Hot Topics in Network, Seattle, WA, USA, 2012
 - 13 Pan J, Paul S, Jain R. A survey of the research on future internet architectures. Communications Magazine IEEE, 2011, 49(7): 26~36
 - 14 <http://www.squid-cache.org>

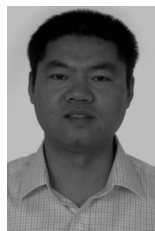
[作者简介]



胡梦春,女,北京交通大学下一代互联网互联设备国家工程实验室硕士生,主要研究方向为异构网络协议兼容机制。



王兆旭,男,北京交通大学下一代互联网互联设备国家工程实验室博士生,主要研究方向为异构网络协议兼容机制、信息中心网络环境下的拥塞控制方案和新网络架构原型系统的部署。



罗洪斌,男,北京交通大学教授、博士生导师、下一代互联网互联设备国家工程实验室副主任,中国通信学会第四届青年工作委员会委员,北京通信学会第八届理事会理事,入选教育部新世纪优秀人才支持计划,并获得国家自然科学基金委优秀青年基金资助。目前主要从事未来互联网体系架构、理论与关键技术的研究,正主持和参与多项国家“973”计划、“863”计划、国家自然科学基金项目。近年来在 IEEE/ACM Transactions on Networking (TON)、IEEE Journal on Selected Areas in Communications (JSAC)、IEEE Network 等本领域顶级期刊与国际会议发表论文 50 余篇。



陈功,男,北京交通大学下一代互联网互联设备国家工程实验室硕士生,主要研究方向为异构网络协议兼容机制和路由设备网络感知机制。