浅析现下DNS新型架构转发和控制分离方案的研究

马惠芳[1]　陈　洁[2]　张丽玲[3]
中国移动通信集团重庆有限公司　重庆市　401121

摘　要：针对目前网络安全、智能、差异化等特点，本文提出了一种新的DNS体系结构，该体系结构具有安全防护能力强，可拓展性好等特点。在DNS体系结构中，增加了以转发和控制为基础的DNS服务管理子系统，并与其它相关运营支持系统协同工作，以达到域名系统的差异化运营、恶意域名防劫持、域名服务资源的灵活调配。

关键词：DNS新型结构；SDN技术；转发；控制分离

Analysis of the current DNS new architecture of the forward and control separation scheme

Huifang Ma[1], Jie Chen[2], Liling Zhang[3]
China Mobile Communication Group Chongqing Co., LTD., Chongqing 401121, China

Abstract: In view of the current network security, intelligence, differentiation and other characteristics, this paper proposes a new DNS architecture, the architecture has strong security protection ability, good scalability and other characteristics. In the DNS architecture, a DNS service management subsystem based on forwarding and control is added, which works together with other related operation support systems to achieve differentiated operation of DNS, anti-hijacking of malicious domain names, and flexible allocation of domain name service resources.

Keywords: DNS new structure; SDN technology; Forward; Control of separation

引言：

DNS是网络服务的出发点和入口，它是网络服务发展的基石，而传统DNS体系结构在网络安全、性能等方面都有很大的问题，并且缺乏差别化的经营能力，难以适应网络业务的迅速发展。在传统DNS体系结构和网络部署中，根据客户端的设定，DNS查询流量被直接传输到指定的DNS服务器上，而经过该网络的网元仅对DNS的请求进行透明转发，从而导致了DNS流量被劫持的危险。另外，DNS域名服务的特点是：具有复杂的逻辑设计、低防护能力和低扩展性。因此，现有的DNS体系结构已不能满足健壮性、安全性和智能化的需求，迫切需要一种能够灵活调配、差异化、智能化的DNS体系结构。软件定义网（SDN）是一项具有划时代意义的技术，它为DNS体系结构的优化提出了新的思路。为了适应网络业务的迅速发展，DNS的安全、差异化、智能化等特点，本文提出了一种新的DNS体系结构。本文主要对这种DNS的新体系结构和网络的部署模式进行了深入的探讨，并给出了相应的应用方案。

一、现行DNS体系结构与问题

DNS系统包括一个高速缓存业务节点和一个被授权的业务节点，一般都是以省级或地区为单位进行集中部署。高速缓存服务节点具有缓存和递归查询两种功能，为了增强系统的安全性，将缓存服务节点的缓存服务器独立于递归服务器，并分别提供缓存和递归查询两种功能。在传统DNS系统的网络部署中，根据用户终端（PC、modem等）所配置的DNS服务器地址，通过用户端直接向目标地址传输DNS查询业务，而中间网络装置仅通过DNS请求业务实现透明转发。在安全、性能、差异经营等方面，传统DNS体系结构和部署都存在着难以解决的问题。

1.安全性问题

①DNS恶意篡改：在未抵达DNS之前，有关网络设备不会检测到用户的DNS请求，而攻击者利用该漏洞，对CPE的DNS进行恶意修改，使用户无法正常上网，从而造成信息泄露和财产损失。②DNS攻击：DNS攻击是近几年来针对DNS的攻击活动（DNS、缓存、DDOS）不

断出现，传统DNS体系结构和网络部署难以应付大量DNS攻击。比如，2009年的“暴风影音”事件，造成中国六省一市的主要网络安全事故。

2.资源调度问题

仅能在服务控制装置（BRAS/SR）中，通过将不同的DNS地址分配给用户，以达到分摊负载的目的，而无法根据每个节点的实际工作状况来进行实时、灵活的调度。

3.差异化的运营能力

传统的DNS系统缺少差异化的智能域名，不能满足网络业务的精细化运营管理需求。

4.系统的性能问题

传统的DNS系统服务器不仅要完成基础解析、域名缓存、域名递归，还要兼顾访问控制、安全防护、业务分析等附加功能，系统设计复杂，功能不清晰，扩展能力差，不能满足网络业务的快速发展。

二、DNS体系结构与基于转发与控制的网络配置

1.SDN技术

SDN这个概念是在学术界产生的，它是美国斯坦福大学Cleanslate研究组所提出的，用于优化和简化网络运行的架构。SDN也被称为“软件定义网络”，正如它的名字所暗示的那样，它可以让网络和软件一样容易被修改，并且可以很容易地适应新的商业环境，从而使网络更加智能化。软件定义网络的核心是对平面模块进行中央控制，即SDN控制器，实现了对分布式控制的分离和中央控制。SDN控制器是整个网络的大脑，可以对其管辖区域的所有设备进行集中控制，而受控制的具有一定控制能力和完全转发能力的网元装置则称为“转发器”。转发器只受SDN控制器的控制，它的传输路径完全取决于SDN控制器的运算产生。SDN控制有三个最基本的特点：控制面板转发面分离，集中控制，开放接口。由于SDN控制器可以利用内部控制程序，为各个开关或路由器等网元装置（或由中央控制器管理的转发器），计算出MPLS路由、组播路由和业务路由等，从而取代了传统的多路由协议。采用这种中央控制技术，可以极大地减少网络中的各种协议的配置和部署，简化网络的结构，同时也大大简化了网络的维护和管理，使得网络的维护和管理变得简单，并且可以降低对维护人员的技术要求，大大降低了网络的维护费用。当一个网络中心控制平面模组单元，通过修改、替换控制控制程序或添加新的软件，可以在需要进行多种网络服务的革新时，实现新的业务。由于新业务的大量需求，需要调整实时路径、灵活的业务控制等，这些都可以通过固件程序实现，而无需对每一个网络单元装置进行升级。从而使新的大型网络服务的部署周期由最初的数年缩减为数星期，乃至数日[1]。

SDN的网络结构可以根据逻辑划分为协同应用层、控制层和转发层三个层次。该体系结构自身被划分为管理层面和转发层面，对应于这三个层次。协作应用层的主要工作就是根据不同的用户需要，开发出不同的应用，也就是所谓的协作级应用。目前主要的协作层次应用有OSS、开放协议等。OSS负责整个网络业务的协作。而Openstack在网络、计算、存储等方面的协同工作。除了这些，还有其他的协同层。用户可以在协同层部署一个安全应用程序，分析网络中的威胁，使用控制层所提供的业务界面，阻止攻击，或将其引入流量净化装置。而网络服务界面的攻击，则是由一个由控制器所提供的网络服务呼叫界面。在协作应用层面，安全级别的APP一般不会在意哪个设备被阻塞，只需要通过一个控制器的服务界面来阻止一种业务；然后，控制器就会向网络的不同边界发送一个流表，以阻止符合这个特性的分组。协同级APP还可以是一种网上销售服务，例如，用户可以通过APP向运营商或服务供应商提出申请，或购买一些实时在线服务。有些OTT公司想要立即在多个数据中心间建立一个特定的带宽，可以按小时计费，也可以按分钟计费，这样就可以定制认证和计费功能。本文给出了一种新的路由模式，并将其用于SDN网。在传统IP网中，除了控制面和转发面外，SDN结构还包括了控制面和转发面。SDN是一种重构了传统网络，旨在使SDN能够编程，软件化，并使网络变得更容易[2]。

2.DNS体系结构的转发与控制分离

为了解决目前DNS系统存在的问题，本文提出一种新的DNS体系结构，该体系结构能够有效地提升系统的容量、差异化能力和安全防护能力，从而能够适应高速发展的网络服务需要。新的DNS服务控制子系统、DNSCacheService和DNS授权ServiceNode构成了DNS体系结构。与传统DNS体系结构不同，DNS系统是通过DNS的服务端来直接面向用户的。业务管理子系统通过对DNS的请求信息进行识别与分析，根据用户、时间、地点、业务、资源等多个维度对其进行预处理，并根据不同的策略，将所处理的数据包发送给适当的DNS服务器。DNS业务控制子系统主要承担DNS业务流量控制，网络安全，节点资源调度，差异化控制。DNS服务控制子系统是以SDN技术为基础，以控制与转发分开的SDN技术为基础，它包括DNS服务控制器和DNS服务转发装置：①DNS服务控制器与DNS服务转发装置通过OpenFlow等协议进行交互，以完成相应的业务策略发布和控制。

DNS服务控制器与DNS网管系统、AAA系统、网络安全系统连接，可以获得DNS服务节点的工作状态、用户信息、DNS地址的黑白名单等信息。②DNS业务控制器是DNS业务转发装置的关键组成部分，它具有定制业务策略、定制安全策略、监控链路状态、流量分配策略、DNS服务节点状态采集和监控等功能。DNS服务转发装置，是DNS新体系结构中的转发层装置，接受DNS服务控制器的控制命令，并根据该命令处理DNS数据流（包括识别、修改、丢弃、重定向、转发等）[3]。

DNSCacheService和DNSCodeServicesCode主要提供域名缓存、递归查询等基本功能，将原有的安全防范、用户分析等非域名解析功能剥离出来，交给DNS业务控制子系统。DNS服务控制子系统、DNS缓存服务节点、DNS授权服务节点与网管系统、AAA系统、网络安全系统等支持业务系统协同工作，实现安全、智能化、差异化、安全的域名解析服务。

3.网络的配置

DNS服务控制子系统由DNS服务控制器、DNS服务转发设备之间通过OpenFlow等协议进行交换，DNS业务转发设备根据业务发展需要在省中心或局域网部署，DNS业务控制器和DNS业务转发设备之间通过OpenFlow等协议进行互通。DNS服务控制器与AAA系统、网管系统、网络安全系统等进行了联网，获取用户属性、DNS服务节点状态、网络安全等信息，并根据多维度的因素，产生相应的策略，分配给DNS服务的转发设备。DNS服务管理系统是由BRAS/SR和DNS服务控制系统通过地道或VPN等方法来实现的。通过BRAS/SR将用户DNS请求的流量统一引入DNS服务中。DNS服务转发装置能够识别DNS请求的流量，并按照DNS服务控制器发布的相应策略，将其发送给相应的DNS服务[4]。

4.DNS中基于转发与控制的典型应用方案

本论文所提出的DNS体系结构具有很大的应用前景，能够迅速地为当前网络的安全、DNS的智能分析、DNS分析、差别化等服务。

4.1域名防窃取

近年来，有许多宽带用户的DNS配置遭到了黑客的攻击，这些黑客利用了宽带路由器的漏洞，对用户的DNS进行了篡改，导致很多用户的正常上网被拉入了不法网站，导致了用户的个人信息泄漏和财产受损。由于DNS的传统体系结构和部署模式，使得用户的DNS请求流直接发送到目标DNS服务器，而不能及时发现和拦截非法的、有风险的DNS业务。DNS服务管理子系统在配置了基于转发与控制的基础上，能够对DNS的请求进行预识别和处理。DNS服务控制子系统判定DNS对报文的目标DNS服务器是否处于非法或恶意的DNSIP地址清单，如果DNS对报文的目标DNS服务器地址进行恶意或非法，那么就会将一个警示页推到这个用户，并引导用户修改所述客户端装置DNS配置。

4.2 DNS服务节点负载分摊

在传统DNS体系结构和网络配置中，采用等值路由等方法来分摊DNS服务器的负载，无法根据DNS服务器的实际情况进行实时调整，并且很难在DNS节点间进行负载分摊。采用转发与控制相结合的DNS新体系结构和网络配置模式，能够有效地利用DNS服务资源进行灵活的调度，不仅可以在DNS中完成对服务器的负载分配，还可以在不同地区之间进行负载分摊和容灾备份。DNS服务管理子系统通过与网络管理系统的接口，实时了解DNS的服务资源状况，并根据需要及时调整DNS的请求消息转发策略，使DNS的服务资源得到了有效的分配。

4.3 DNS智能解析与差异化服务

基于转发与控制的DNS体系结构，在现有网络中部署后，DNS业务管理子系统能够根据用户属性、时间、基站、业务等多个方面的策略因素，制订DNS查询消息转发策略，并与DNS服务节点合作，实现域名智能解析、差异化域名解析。

三、结束语

本文从安全、性能、安全等方面对当前网络域名体系结构和配置方式进行了研究，并在此基础上提出了一种新的基于转发和控制的DNS服务控制系统。采用分布式的DNS体系结构，能够灵活调度DNS节点资源、域名解析差异化、DNS流量防劫持等功能，极大地提高了运营商的网络服务提供能力和防御网络攻击的能力，为广大用户提供安全、可靠的互联网服务。

参考文献：

[1]彭巍，贺晓东，李韶英，等.基于SDN架构的DNS流量调度方法研究[J].广东通信技术，2022，42（2）：59-62.

[2]常朝稳，金建树，韩培胜，等.基于属性签名标识的SDN数据包转发验证方案[J].通信学报，2021，42（6）：131-144.

[3]祝现威，常朝稳，朱智强，等.基于身份属性的SDN控制转发方法[J].通信学报，2019，40（11）：1-18.

[4]李妍星.DNS安全扩展与可扩展分布式DNS研究[D].四川：电子科技大学，2021，52（4）：773-781.