(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110730252 A
(43)申请公布日 2020.01.24

(21)申请号 201910908679.7

(22)申请日 2019.09.25

(71)申请人 南京优速网络科技有限公司
地址 210000 江苏省南京市江宁经济开发区秣周东路12号悠谷2号楼1503室

(72)发明人 黄韬 汪勇 吴兴利 周梅岚 戴云伟

(74)专利代理机构 江苏圣典律师事务所 32237
代理人 贺翔

(51)Int.Cl.
H04L 29/12(2006.01)
H04L 29/08(2006.01)
H04L 12/741(2013.01)

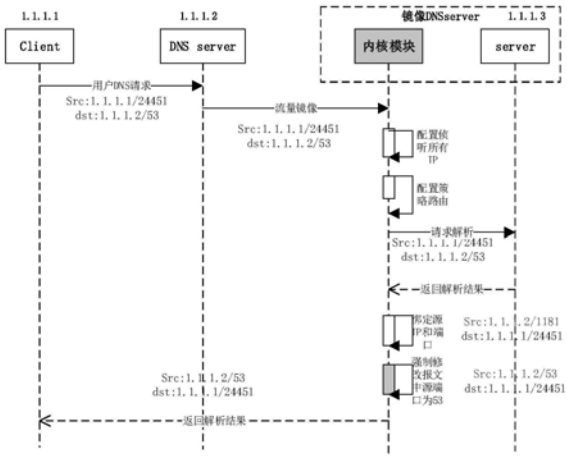
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种通过改造linux内核报文处理功能的地址转换方法

(57)摘要

本发明提供一种通过改造linux内核报文处理功能的地址转换方法，其原理是通过配置socket的IP_TRANSPARENT选项，设置DNS服务程序侦听所有的IP地址(包括非本机地址)，再通过策略路由的方式将所有请求送至应用层进行正常解析，在回复用户时将源地址强制绑定为原DNS服务器的IP，端口信息则通过改造内核模块进行二次绑定，最终返回报文源IP地址为原DNS服务器，端口为53，完成透明的代理功能。利用内核模块本身的处理能力，无需维护巨大的地址转换表，从而提升了数据传输性能，解决了因网络地址转换的造成的DNS服务性能瓶颈问题。



CN 110730252 A

1.一种通过改造linux内核报文处理功能的地址转换方法,其特征在于,所述地址转换方法包括以下步骤:

步骤1:镜像节点配置socket的IP_TRANSPARENT选项,使服务程序监听所有的IP地址;

步骤2:将镜像节点接收到的DNS请求消息策略路由至local发送至应用层;

步骤3:镜像节点服务程序正常解析;

步骤4:镜像节点将解析结果进行封装,绑定源IP为1.1.1.2、源端口为特定端口;

步骤5:先将绑定的特定源端口强制修改为指定编号;

步骤6:将封装好的消息返回至发送DNS请求终端。

2.根据权利要求1所述的一种通过改造linux内核报文处理功能的地址转换方法,其特征在于,

所述步骤5,通过内核模块来执行,所述内核模块为:DNS端口赋值内核模块。

3.根据权利要求1所述的一种通过改造linux内核报文处理功能的地址转换方法,其特征在于,

所述步骤4中的特定源端口指1181,所述步骤5中,特定源端口1181强制修改为53。

一种通过改造linux内核报文处理功能的地址转换方法

技术领域

[0001] 本发明涉及互联网通信技术领域，尤其是涉及一种通过改造linux内核报文处理功能的地址转换方法。

背景技术

[0002] 域名系统(Domain Name System，简称DNS)是互联网的基础设施和“神经中枢”系统，支撑着互联网的正常运转。保障域名系统的安全，是保障互联网安全的先决条件。为强化我国域名服务的安全性和稳定性，通过建设镜像DNS节点(根、顶级域、权威域等)的方式加强互联网域名的监测和安全管控。

[0003] 镜像服务需要将请求消息的目的地址转换为镜像DNS节点，返回消息的源地址转换为原DNS服务器地址送至客户端。现有方案是通过NAT技术的来实现，具体过程如图1所示。

[0004] 现有技术是利用NAT技术将请求的目的地址转换为镜像DNS节点，返回至终端用户时需要将源地址转换为DNS节点的地址。但DNS的请求量可达百万级QPS以上，基于NAT技术就需要在内存中维护一张巨大的NAT地址表，并进行频繁的读写操作，大大降低了发送数据的效率，导致大量的丢包，影响镜像DNS节点的服务性能。

发明内容

[0005] 针对上述技术问题，本发明提供了一种基于传输层信息控制的地址和端口转换方式，利用内核模块本身的处理能力，无需维护巨大的地址转换表，从而提升了数据传输性能，解决了因网络地址转换的造成的DNS服务性能瓶颈问题。

[0006] 本方案的原理是通过配置socket的IP_TRANSPARENT选项，设置DNS服务程序侦听所有的IP地址(包括非本机地址)，再通过策略路由的方式将所有请求送至应用层进行正常解析，在回复用户时将源地址强制绑定为原DNS服务器的IP，端口信息则通过改造内核模块进行二次绑定，最终返回报文源IP地址为原DNS服务器，端口为53，完成透明的代理功能。

[0007] 步骤1:镜像节点配置socket的IP_TRANSPARENT选项，使服务程序监听所有的IP地址(包含非本机的IP)

[0008] 步骤2:将镜像节点接收到的DNS请求消息策略路由至local，送至应用层；

[0009] 步骤3:镜像节点服务程序正常解析；

[0010] 步骤4:镜像节点将解析结果进行封装，强制绑定源IP为1.1.1.2，源端口为某个特定端口，如1181；

[0011] 步骤5:通过自主研发的内核模块先将绑定的特定源端口1181强制修改为53；

[0012] 步骤6:将封装好的消息返回至终端1.1.1.1。

[0013] 本发明具有如下有益效果：

[0014] 现有的NAT技术在解决了地址转换的问题，但随着DNS请求量的增大，维护NAT地址表会影响数据的传输效率，产生响应时延增大、丢包等现象，成为镜像DNS服务的性能瓶颈。

[0015] 本发明技术方案通过改造linux的内核模块,在报文处理过程中完成地址和端口的绑定,减少地址转换的资源开销。具体有以下优势:

[0016] 1、提高传输效率:通过自主研发的内核模块利用系统本身的报文处理过程实现高效的地址转换,无需维护巨大的NAT地址表,减少了系统资源的消耗,降低时延,提升了数据的传输效率

[0017] 2、提升镜像DNS的服务性能:同等配置下,镜像DNS服务性能从10万QPS提升至百万级QPS。

附图说明

[0018] 图1为现有技术中的源地址转换方法流程示意图;

[0019] 图2为本发明源地址转换方法流程示意图。

具体实施方式

[0020] 现将结合附图对本发明的技术方案进行完整的描述。以下描述仅仅是本发明的一部分实施案例而已,并非全部。基于本发明中的实施案例,本领域技术人员在没有作出创造性劳动的前提下所获得的所有其他实施案例,都属于本发明的权利保护范围之内。

[0021] 本提案的关键点是提出一种通过改造linux内核模块在报文处理过程中完成非本机IP地址和端口的绑定,最终实现镜像DNS的正常应答。本提案也适用于有相同地址转换业务需求的场景,本提案欲保护的点如下:

[0022] 1、本提案提出利用socket的IP_TRANSPARENT配置侦听所有IP的消息,并通过策略路由的方式将非发往本机的请求送至应用层。

[0023] 2、本提案中的返回消息则是将源IP强制bind为原DNS服务器IP地址

[0024] 3、53端口已被DNS服务占用,本提案中通过内核模块处理,先绑定一个特定的端口号,再通过二次绑定,将特定端口修改为53,将返回消息发送至终端。

[0025] 实施例1

[0026] 本方案的原理是通过配置socket的IP_TRANSPARENT选项,设置DNS服务程序侦听所有的IP地址(包括非本机地址),再通过策略路由的方式将所有请求送至应用层进行正常解析,在回复用户时将源地址强制绑定为原DNS服务器的IP,端口信息则通过改造内核模块进行二次绑定,最终返回报文源IP地址为原DNS服务器,端口为53,完成透明的代理功能。

[0027] 步骤1:镜像节点配置socket的IP_TRANSPARENT选项,使服务程序监听所有的IP地址(包含非本机的IP)

[0028]
```
int opt =1;
setsockopt(server_socket,SOL_IP, IP_TRANSPARENT,&opt,sizeof(opt));
```

[0029] 步骤2:将镜像节点接收到的DNS请求消息策略路由至local,送至应用层

[0030]
```
ip route add local 0.0.0.0/0    dev lo table tablename
```

[0031] 步骤3:镜像节点服务程序正常解析

[0032] 步骤4:镜像节点将解析结果进行封装,强制绑定源IP为1.1.1.2,源端口为某个特

定端口，如1181，当前这台机器的53端口已经被占用，无法绑定给1.1.1.2，所以需要先绑定一个特定端口，这个端口可以自定义，只要不冲突。

[0033] 步骤5：通过自主研发的内核模块先将绑定的特定源端口1181强制修改为53，自主研发的内核模块为DnsPortAssignment.ko，该模块就是将这个特定的源端口强制修改为53后送出，53端口为DNS协议的端口号，必须是这个53端口号，终端才能识别。本身linux内核没有这个功能。

[0034] 这个内核模块完成的功能为绑定特定的端口，再送出前再修改为53，

[0035] 步骤6：将封装好的消息返回至终端1.1.1.1。

[0036] 以上实施例仅供说明本发明之用，而非对本发明的限制，有关技术领域的技术人员，在不脱离本发明的精神和范围的情况下，所作出各种变换或变型，均属于本发明的范畴。

[0037] 以上显示和描述了本发明的基本原理、主要特征和本发明的优点。本行业的技术人员应该了解，本发明不受上述实施例的限制，上述实施例和说明书中描述的只是说明本发明的原理，在不脱离本发明精神和范围的前下，本发明还会有各种变化和改进，本发明要求保护范围由所附的权利要求书、说明书及其等效物界定。

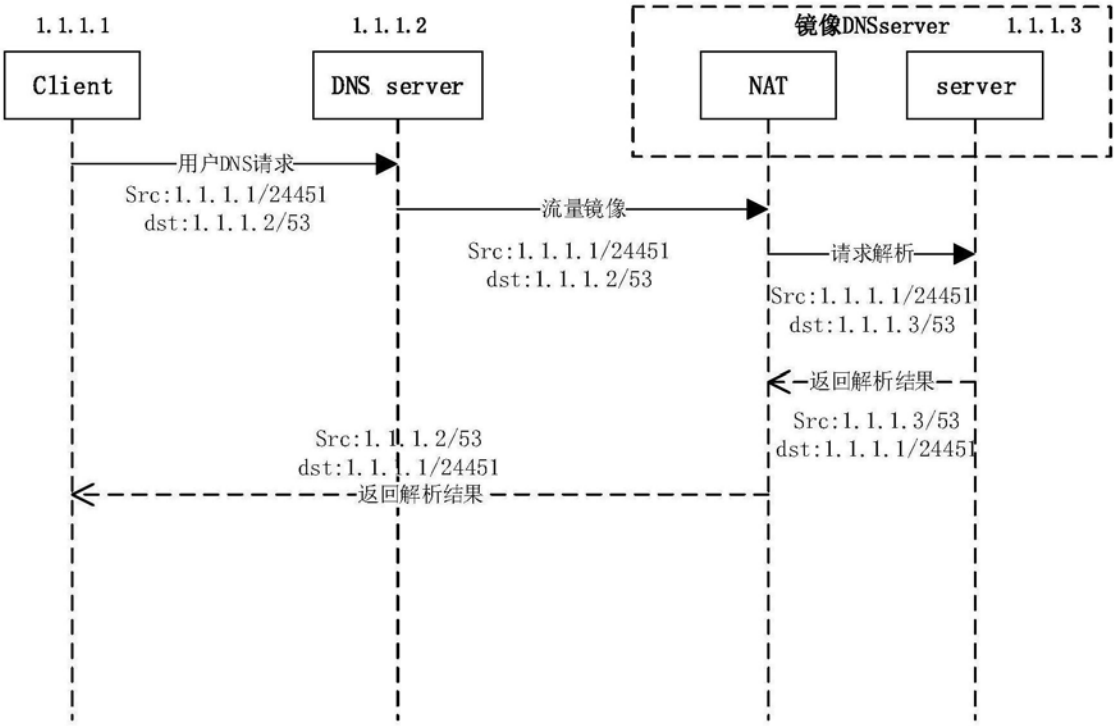

1.1.1.1
1.1.1.2
镜像DNSserver
1.1.1.3
Client
DNS server
NAT
server
用户DNS请求
Src:1.1.1.1/24451
dst:1.1.1.2/53
流量镜像
Src:1.1.1.1/24451
dst:1.1.1.2/53
请求解析
Src:1.1.1.1/24451
dst:1.1.1.3/53
返回解析结果
Src:1.1.1.3/53
dst:1.1.1.1/24451
Src:1.1.1.2/53
dst:1.1.1.1/24451
返回解析结果

图1

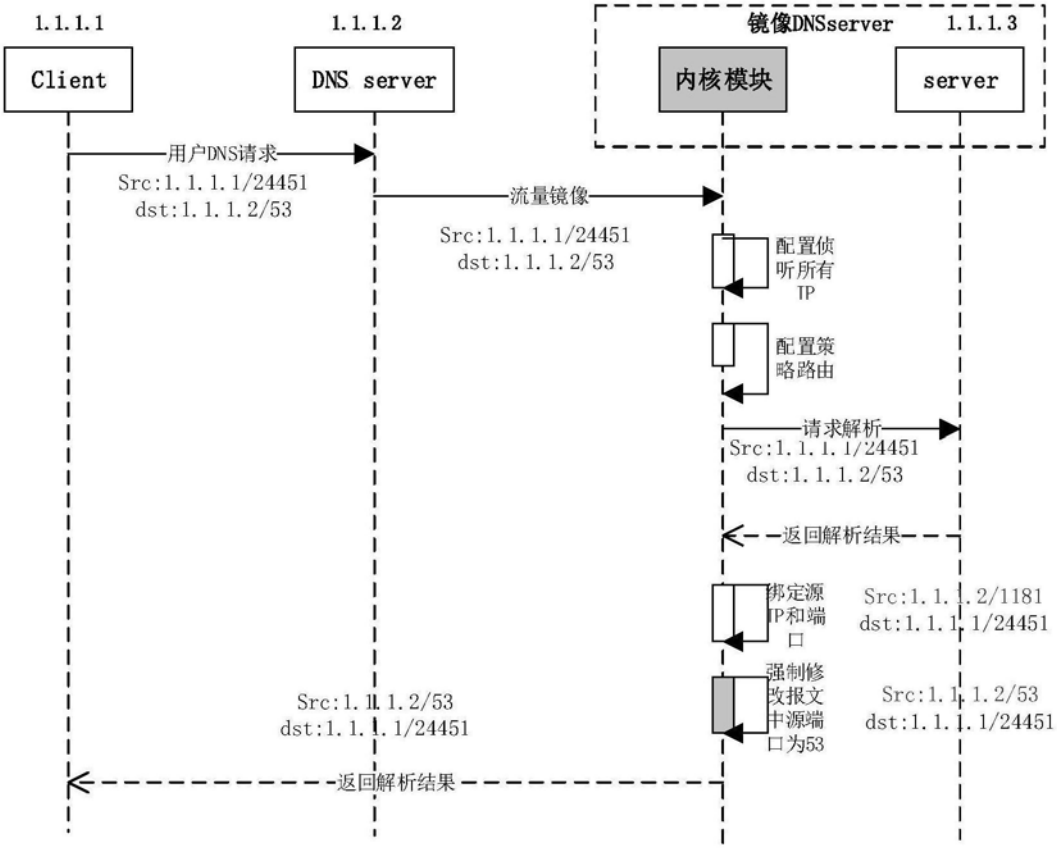

1.1.1.1
1.1.1.2
镜像DNSserver
1.1.1.3
Client
DNS server
内核模块
server
用户DNS请求
Src:1.1.1.1/24451
dst:1.1.1.2/53
流量镜像
Src:1.1.1.1/24451
dst:1.1.1.2/53
配置侦听所有IP
配置策略路由
请求解析
Src:1.1.1.1/24451
dst:1.1.1.2/53
返回解析结果
绑定源IP和端口
Src:1.1.1.2/1181
dst:1.1.1.1/24451
强制修改报文中源端口为53
Src:1.1.1.2/53
dst:1.1.1.1/24451
Src:1.1.1.2/53
dst:1.1.1.1/24451
返回解析结果

图2