



面向 C2C 通信的轻量级 TURN 实现架构及方案

王爱俊¹, 刘冰²

(1. 中国电信股份有限公司北京研究院 北京 100035;

2. 华为技术有限公司北京研究所 北京 100095)

摘要:提出了一种适用于复杂网络环境下 C2C 通信的轻量级 TURN (TURN-Lite) 实现架构及方案。本架构及方案可大幅简化当前业界所采用的 TURN 实现流程, 充分利用现网已经大量部署的分布式数据中转设备 (如 CGN/CDN) 的数据转换和中转能力, 实现网络能力的对外开放, 为 C2C 通信应用开发商提供高效的数据中转服务。

关键词: TURN; 轻量级 TURN; C2C 通信

doi: 10.11959/j.issn.1000-0801.2015262

Architecture and Solution of Lightweight TURN for C2C Communication

Wang Aijun¹, Liu Bing²

(1. Beijing Research Institute of China Telecom Co., Ltd., Beijing 100035, China;

2. Beijing Research Institute of Huawei Technologies Co., Ltd., Beijing 100095, China)

Abstract: An architecture and solution of lightweight TURN (TURN-Lite) which was suitable for C2C communication scenarios in complex network environment was described. It could simplify the communication processes used by current TURN solution and made full use of the data conversion and transfer capability of distributed data transfer devices (such as CGN/CDN) which had already deployed in current network, opened up network capabilities and provided efficient data transfer services for C2C communication applications developers.

Key words: TURN, lightweight TURN, C2C communication

1 引言

随着智能硬件以及物联网相关业务的兴起, 传统的以获取信息为主的 C/S 通信模式正在向 C/C 通信模式转变。人与人、人与物、物与物之间的通信需求加速了业界对 C2C 通信方式的研究。考虑到现网网络环境的复杂性, 尤其是从家庭网关到网络设备间大量 NAT 设备的存在, 业

界在实现 C2C 通信时, 采用的方案一般是通过云端集中转发, 即通信双方都连接到一个中转点, 由应用层来实现数据的中转服务。这样就造成了各个应用开发商在业务部署时, 均需部署自己的数据中转服务器, 业务服务器到中转服务器之间没有通用的标准, 不同中转服务器间的能力无法共用。如果业务提供者部署的中转服务器覆盖范围不足, 则会造成 C2C 通信的路径绕转, 时延增加。

收稿日期: 2015-06-02; 修回日期: 2015-10-10

论文引用格式: 王爱俊, 刘冰. 面向 C2C 通信的轻量级 TURN 实现架构及方案. 电信科学, 2015262

Wang A J, Liu B. Architecture and solution of lightweight TURN for C2C communication. Telecommunications Science, 2015262



图1显示了针对智慧家庭业务部署时,基于业界当前实现方案的部署现状。当用户购买多个厂商的智能设备时,如果想远程控制这些智能设备,一般均需要通过各厂商自己部署的TURN服务器,实现复杂NAT穿越和数据中转。

而另一方面,运营商在现网已经部署了大量的CGN/CDN设备,这些设备的最主要功能就是完成公私网之间通信所需的NAT及数据中转。如果能利用这些网络设备的能力,完成在复杂网络环境下,C2C设备间的NAT和数据中转,就会大幅降低各类C2C应用开发商务部署的难度,提升其业务部署、扩容速度和C2C通信效率。从C2C通信的使用者来看,其设备之间的通信无需再通过各类设备厂商自己部署的中转服务器,而是通过不感知业务内容的网络设备,其通信私密性也会大大加强。典型的如远程视频监控业务、基于云平台的家庭视频监控始终存在云平台被滥用而导致隐私泄露的风险。

2 业界TURN解决方案存在的不足

业界当前应对复杂网络环境下的C2C通信解决方案主要是TURN(RFC5766),但TURN解决方案存在如下不足。

(1)TURN与ICE紧耦合

TURN实现方案中,要求每个通信方都要从TURN服务器处获取自己的中继地址,之后的数据中转将通过中继

地址来实现。在对称NAT网络环境下,针对不同的目标公网地址,NAT设备会将同一源地址映射为不同的反射地址(reflex address)。这样,当通信一方将数据发往对端中继地址时,由于针对该中继地址形成的反射地址不同于通信对方之前针对TURN服务器的well-known地址在NAT设备上形成的映射表项,发往对端中继地址的数据将被通信对方的对称NAT设备丢弃。

为保证通信的可靠性,TURN解决方案还需要额外的NAT设备穿越信令(如基于ICE中的地址通信探测流程)来实现针对中继地址的NAT穿越,造成TURN与ICE解决方案的紧耦合。

(2)TURN服务器需要预留大量的中继地址

TURN解决方案要求为每个通信方都分配不同的中继地址,这就要求在TURN服务器上预留大量的IPv4、IPv6公网地址块。当TURN服务器采用分布式部署时,由于难以确定每个TURN服务器上连接的客户数量,会造成这些公网地址的浪费,加剧了IPv4地址的短缺。

(3)TURN服务器需要同时开启大量的TCP/UDP连接

TURN解决方案要求为每个客户的UDP连接,在TURN服务器上需要保存实时的session连接,大量客户同时连接时,就需要有大量的UDP session同时在线。而针对TCP通信需求,现有的TURN解决方案要求针对一个客户方要维持两个TCP连接,这更加剧了TURN服务器的压力,同时也使得该方案很难集成到现有的网络设备当中。

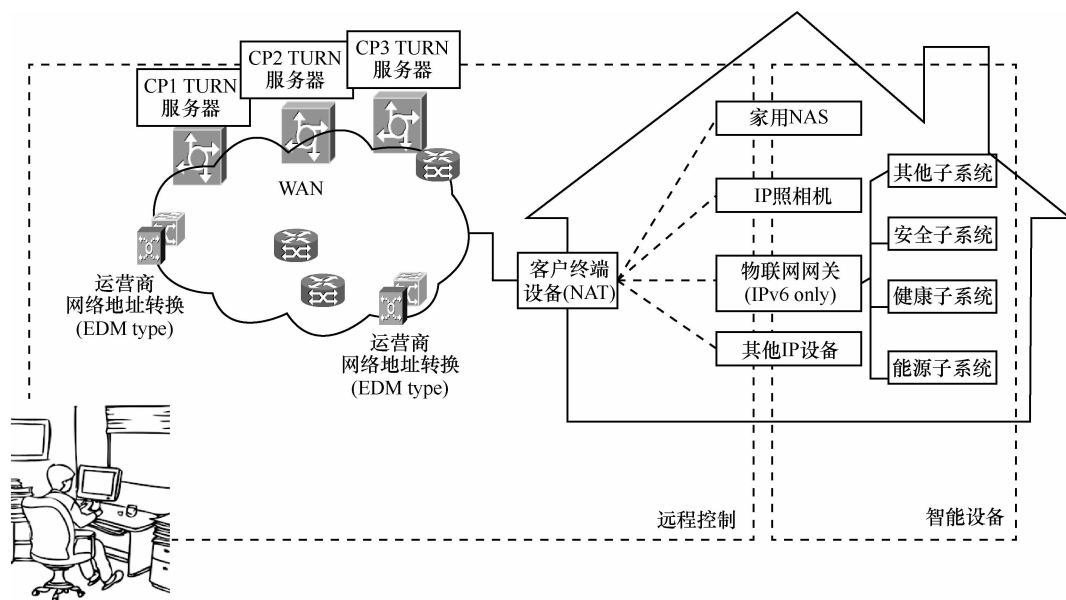


图1 C2C通信实现现状示例(智慧家庭)

(4) 采用了不同流程实现 TCP、UDP 数据中转

针对通信双方的 TCP 或 UDP 通信需求,TURN 采用了不同的流程来实现数据的中转。这就使得应用开发商在集成 TURN 解决方案时,需要有不同的集成方案来实现 TCP/UDP 之间的数据中转,增加了其应用实现的难度。

(5) TURN 服务器之间的数据中转实现复杂

在当前的 TURN 实现方案中,由客户端自行完成 TURN 服务器的选择。如果通信双方选择了不同的 TURN 服务器,则需要实现在 TURN 服务器之间的数据中转。RFC5766 还没有涉及不同 TURN 服务器间的数据中转。要实现 TURN2TURN 的数据中转,需要再增加额外的 STUN 属性,以携带不同的 TURN 服务器所分配的中继地址,同时还需要解决 TURN 服务器针对这些中继地址的可靠性问题。

3 TURN-Lite 架构总述

针对现有解决方案的上述不足,本文提出了一种轻量级 TURN(TURN-Lite)的解决方案,其所采用的架构如图 2 所示。其中采用现网分布部署的网络设备(以 CGN 为例,基于 CDN 设备的实现与此类似)实现数据中转和 NAT 的功能。为了实现对这些分布部署的 TURN-Lite 设备的集中管控,将这些设备的能力以统一接口的方式提供给各类 App 开发商,新增了 RS(relay selector)设备,通过它完成对

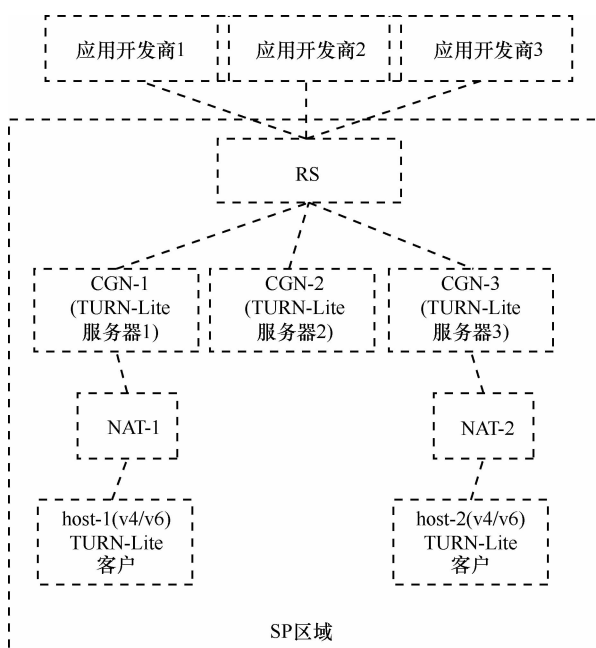


图 2 轻量级 TURN(TURN-Lite)实现架构示意

TURN-Lite 设备的优化选择。

应用开发商在采用 TURN-Lite 方案时,调用运营商提供的中转服务实现其客户端间或者客户端到其设备间的远程通信时,所需的关键环节描述如下。

(1) RS 选择和反射

当运营商部署多个 RS,或者应用的通信双方分布在不同的运营商时,应用开发者首先要选择一个合适的 RS,由其完成对其所控制的中继设备的选择。

通信双方在获得 RS 服务器的地址后(一般由应用服务器在其登录注册时返回),就向该 RS 发送 STUN 消息,获取其针对该 RS 地址的反射地址(后续简称为 reflex-RS),并将其上报给应用服务器(App server)。

(2) 中继设备选择

应用服务器将通信双方的 reflex-RS 通过开放的接口发送给 RS,由 RS 依据通信双方的 reflex-RS 地址为通信双方选择合适的中继设备。

当通信双方位于同一个运营商内时,中继设备的选择原则还可以基于其他的标准,如通信双方通信路径上的链路利用率,以保证用户到该中继设备的时延最小。另外可以考虑通信双方是否有隐私保护需求,如有,则可以选择离通信双方较远的中继设备来完成数据中转,避免通信一方根据中继地址分析出对端所处位置等。

如通信双方位于不同的运营商内,采用本方案亦可实现复杂网络环境下的端到端通信。不过由于 RS 只掌握一方运营商的网络状况,所选择的中继设备可能会损失一些通信效率。针对这种场景,另一种可行的解决方案是应用服务器同时与两个运营商的 RS 通信,由各自的 RS 完成本域内最优中继设备的选取,数据中转通过两个中继设备来完成。

(3) “couple”命令生成和下发

通信双方在获取到其间通信所用的中继设备 well-known 地址后,均向该 well-known 地址来发送 STUN 消息,获取其针对该中继 well-known 地址的反射地址(后续简称为 reflex-relay),并连同之前获得的 reflex-RS 地址,一并发给 RS。

RS 从 App provider 获取到通信双方的 reflex-RS 地址,根据对应关系,即可找到待通信双方的 reflex-relay 地址。基于该 reflex-relay 地址对以及通信双方拟采用的传输层协议(TCP 或者 UDP),就可形成“couple”命令并下发给对应的中继设备。



(4)数据中转

通信双方此时就可以开始通过中继设备进行数据的传输。与 TURN 解决方案不同的是,TURN-Lite 设备无需给每个通信方分配不同的中继地址,它们均采用已选择中继设备的 well-known 地址进行通信,这就避免了在第 3 节中提到的,现有 TURN 解决方案的诸多问题。

当通信一方将数据发送给已选择中继设备的 well-known 地址后,其数据分组的源地址会被 NAT 设备转换为 reflex-relay 地址,中继设备在接收到该数据分组后,依据 RS 发送给中继设备的 couple 命令,将该数据分组的目的地地址替换成 couple 命令中所指定的另一端设备的 reflex-relay,该数据分组的源地址替换成中继设备的 well-known 地址,转换后的数据将顺利通过通信对方的所有 NAT 设备,最终达到通信对端。

返回的数据分组在经过中继设备时,做类似的处理。这样就实现了通信双方的数据中转通过公用的第三方来完成的目标。应用开发者在业务规模扩大时就无需再考虑如何快速部署其数据中转服务器,可以顺利地将给基本的数据中转需求转分组给运营商或者其他第三方服务提供者。

4 CGN/CDN 设备接口描述 (couple)

为充分利用现网已大量部署的 CGN/CDN 设备在数据转换及中转方面的能力,TURN-Lite 架构定义了一个同时

适用于 TCP、UDP 数据转发的标准控制接口。基于本接口,CGN/CDN 设备只需接收从 RS 发来的映射指令 (couple 命令),就可以按照映射指令所要求的内容对后续的数据进行 NAT 和中转传递。

couple 接口的报文接口如图 3 所示,采用了与 STUN message 相同的封装方式,在数据报文中封装了 STUN 当前定义的一些属性(attribute)。

其中 STUN 消息格式、长度、短报文数据、交易 ID 与现有 STUN message 的定义基本一致。关键是本报文中携带的后续 3 个属性。

- XOR-Mapped-Address: 封装了通信终端相对于中继的反射地址,即 reflex-relay。
- XOR-Peer_Address: 封装了通信对端相对于中继的反射地址,通信对端的 reflex-relay。
- Requested-Transport: 封装了通信双方所使用的传输层协议(TCP 或者 UDP)。

在 CGN/CDN 设备上,依据上述接口将形成类似表 1 的映射表。

表 1 CGN/CDN 设备上的映射表结构

host-1 的反射地址 (针对中继设备)	host-2 的反射地址 (针对中继设备)	传输协议
192.0.2.1:7000	202.0.2.150:32101	TCP
..*.*	*.*.*.*	UDP



图 3 CGN/CDN 接口 couple 指令格式

基于本接口,CGN/CDN 等中继设备只需在其本身的 well-known 地址上侦听来自客户端的 TCP、UDP 数据,依据接收到数据的源地址和传输协议来判断。

如果 couple 指令形成的映射表中,存在该数据源地址/传输协议对应的表项,则按照如下规则进行处理。

- 将该数据的源地址转换为本中继设备的 well-known 地址。
- 将该数据的目的地址转换为映射表中对应的通信对端的 reflx-relay 地址。
- 重新计算 TCP、UDP 数据分组的校验和。

如果 couple 指令形成的映射表中,不存在该数据源地址对应的表项,则将该数据丢弃。返回的数据分组按照同样的规则进行处理。

5 TURN-Lite 优势

相比于 TURN,TURN-Lite 具有如下的优势。

(1)与 ICE 解耦

由于客户端与中继设备的信令通信端口与数据通信端口相同,客户端在向中继设备发送STUN binding 请求,获取针对该中继 well-known 地址的反射地址时,就在沿途的 NAT 设备上形成了相应的映射表项,为后续从该端口接收数据做好了准备。无需像 TURN 当前解决方案所要求的,还需要类似 ICE 等其他 NAT 打洞信令。

这样,实现了数据中转与 ICE 等协议的解耦,简化了其实现过程。

(2)更少的地址/端口消耗和管理

TURN-Lite 架构中,所有的通信终端均与中继设备的 well-known 地址通信,中继设备无需为每个通信终端分配中继地址,这就极大地减轻了中继设备对公网 IPv4/IPv6 地址的消耗和管理,使得该方案很容易以分布式方式广泛部署。

(3)简化的实现流程

与现有 TURN 方案中需要超过 8 个命令来实现数据中转不同,TURN-Lite 理论上仅需两个命令就可以完成相关的中继功能。表 2 是当前 TURN 与 TURN-Lite 实现相关数据转发所需的命令对比。

另外,TURN 当前的解决方案针对 TCP、UDP、IPv4/IPv6 终端间的通信采用了不同的流程,而 TURN-Lite 如前所述,则采用了统一的方式来处理各类终端间的 TCP、UDP 通信。

表 2 当前 TURN 与 TURN-Lite 实现相关数据转发所需的命令对比

	TURN 解决方案	TURN-Lite 解决方案
所需命令	binding; allocate; send; data; channel bind; connect; connect bind; connection attempt	binding; couple

(4)支持优化的中继设备选择

TURN 解决方案中,由各通信终端来进行 TURN 服务器的选择,在 TURN-Lite 解决方案中,则采用通过集中选择中继的方式(relay selector)来实现合理的数据中转点,这样后续数据的中转就可以避开一些拥塞的链路。另外,集中选择中继的方案还可以考虑其他一些中继选择因素,如因通信过程保密而选择一些较远的中继,以避免通过中继 IP 地址来判断通信方所处位置等。

6 TURN-Lite 部署考虑

TURN-Lite 最适合以分布的方式进行部署。现网中最适合集成 TURN-Lite 方案的网络设备是已大量部署的 CGN/CDN 设备。集成了 TURN-Lite 方案的 CGN/CDN 设备可实现数据的分布式优化转发,为大量的 C2C 应用开发者提供通用的、标准化的数据中转服务,减轻 C2C 应用开发者在业务规模发展时的中转服务器部署瓶颈,同时也能最大限度地发挥网络设备的对外开放能力。

7 TURN-Lite 方案验证

基于 TURN-Lite 方案,开发并试验了相应的原型系统。原型系统通信采用的网络拓扑如图 4 所示。

基于该原型验证系统,实现了位于对称 NAT 后的 IPv4 设备间通信以及 IPv4 终端与 IPv6 终端间的通信,验证了 DS-Lite 方案的可行性。

在图 7 中,DSR master/slave 承担了 RS(relay selector)的角色,Mrelay 则承担了 TURN-Lite 服务器的角色。其中 IPv4 终端与 IPv6 终端间通信过程如图 5 所示。

8 结束语

本文提出的 TURN-Lite 解决方案大幅简化了业界常用的 TURN 解决方案,使数据的中转服务很容易集

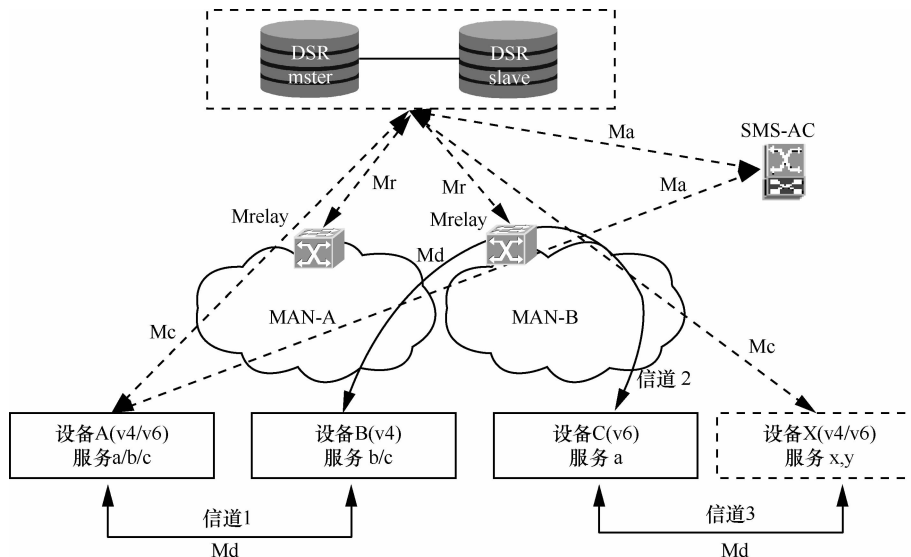


图4 TURN-Lite 方案验证原型系统

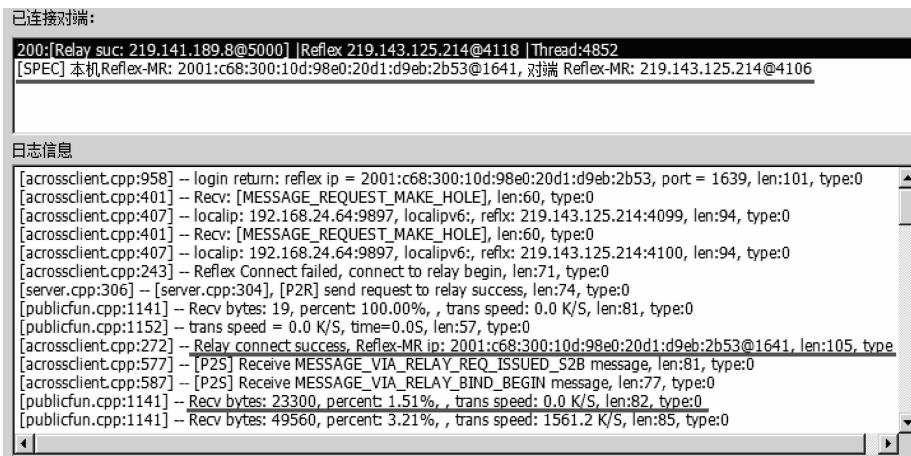


图5 IPv4 终端与 IPv6 终端基于 TURN-Lite 方案的通信验证

成到现网已经大量部署的 CGN/CDN 设备中,一方面可充分发挥现网网络设备的对外服务能力,另一方面可优化 C2C 通信的效率,提升 C2C 应用开发者业务规模部署的能力,减轻其在业务规模部署时所遇到的中转服务器瓶颈问题。

参考文献

- 1 RFC6156. Traversal Using Relays Around NAT (TURN) Extension for IPv6, 2011
- 2 RFC6144. Framework for IPv4-IPv6 Translation, 2011
- 3 RFC6146. Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers, 2011
- 4 RFC6062. Traversal Using Relays Around NAT (TURN) Extensions for TCP Allocations, 2010

[作者简介]



王爱俊,男,中国电信股份有限公司北京研究院高级工程师,从事 IP 网络技术研究工作,主要研究方向为流量优化、IP 网络能力开放及智能化、基于 SDN 的网络能力实现等,已申请并授权 7 项专利。



刘冰,男,博士,华为技术有限公司北京研究所研究员,从事网络技术研究、通信、IP 标准化工作,已在 IETF、ITU-T 等国际标准组织参与发表多篇标准文案。